Warranty Registration
Register online today for a chance to win a FREE Tripp Lite product! www.tripplite.com/warranty

Owner's Manual

IP Remote Access Unit
Model #: B050-000

LISTED 1F61 I.T.E.

N14663

About the B050-000

The B050-000 provides remote KVM access and control. You can use the B050-000 to manage and monitor components in your servers through a modem or LAN, even if your network is down. The B050-000 offers a comprehensive hardware solution for server management.

Technical Support

If you need help installing, configuring or running the B050-000 IP Remote Access Unit, call a Tripp Lite Technical Support Representative at (773) 869-1234 or visit Tripp Lite's website at: www.tripplite.com

Tripp Lite World Headquarters
1111 W. 35th Street, Chicago, IL 60609 USA
(773) 869-1234 • www.tripplite.com

Note: Follow these instructions and operating procedures to ensure correct performance and to prevent damage to this unit or to its connected devices.

Copyright © 2006 Tripp Lite. All rights reserved. All trademarks are the property of their respective owners.
The policy of Tripp Lite is one of continuous improvement. Specifications are subject to change without notice.

Table of Contents

1. Quick Start Guide **3**
- Installation 3
- Connectors and Indicators 3
  - General Overview 3
  - Front Side Connectors (Figure 1-2) 4
  - Rear Side Connectors (Figure 1-3) 5
- Connecting the B050-000 to the Host System 5
- Initial Network Configuration 6
- B050-000 Setup Tool 6
  - Main Window 6
  - MAC Address Detection 7
  - Authentication 8
- Configuration via Serial Interface 8
- Web Interface 9
- The Remote Console 9

2. Introduction **11**
- Features 11
- B050-000 System Components 12
- When the Server is Up and Running 12
- When the Server is Dead 12

3. Installation **14**
- Operation Overview 14
- Connectors and Indicators 14
  - General Overview 14
  - Front Side Connectors and Indicators 15
  - Rear Side Connectors 16
- Connecting the B050-000 to the Host System 16
- Connecting a Local Console 17
- Connecting Ethernet 17
  - 10 Mbps Connection 17
  - 100 Mbps Connection 17

4. Configuration **18**
- Initial Configuration 18
- B050-000 Setup Tool 18
  - Main Window 18
  - MAC Address Detection 19
  - Authentication 20
- Initial Configuration via DHCP Server 20
- Initial Configuration via Serial Console 21
- Web Interface 21
- Mouse, Keyboard and Video configuration 22
  - B050-000 USB Interface 22
  - B050-000 Keyboard Settings 22
  - Remote Mouse Setting 22
  - Auto Mouse Speed 22
  - Fixed Mouse Speed 23
  - Single/Double Mouse Mode 23
- Auto Mouse Speed and Mouse Synchronization 23
  - Host System Mouse Settings 24
  - Single and Double Mouse Mode 24
  - Recommended Mouse Settings 24
  - Video Modes 25
- Resetting the B050-000 to its Factory Settings 25
  - Using the Serial Interface 25

5. Usage **26**
- Prerequisites 26
- Login to the B050-000 and Logout 27
  - Login to the B050-000 27
  - Navigation 28

5. Usage (continued)
  - Logout from the B050-000 29
- The Remote Console 30
  - General Description 30
  - Main Window 30
  - Optimizing the Video Picture 42
  - Reducing the Noise of the Video Picture 42
  - Using the B050-000 with Low Bandwidth 43

6. Menu Options **44**
- Remote Control 44
  - KVM Console 44
  - Remote Power 45
  - Telnet Console 46
- Virtual Media 47
  - Floppy Disk 47
  - CD-ROM 49
  - Drive Redirection 52
  - Options 58
  - Creating an Image 58
- User Management 61
  - Change Password 61
  - Users And Groups 62
- KVM Settings 63
  - User Console 63
  - Keyboard/Mouse 67
  - Video 69
- Device Settings 69
  - Network 69
  - Dynamic DNS 73
  - Security 75
  - Certificate 76
  - Serial Settings 78
  - Intelligent Platform Management Interface (IPMI) 80
  - Date And Time 81
  - Event Log 82
- Maintenance 84
  - Device Information 84
  - Event Log 85
  - Update Firmware 86
  - Unit Reset 87

Appendices **88**
- A. Frequently Asked Questions 88
- B. Glossary 90
- C. B050-000 Video Modes 92
- D. Users and Roles 93
- E. Key Codes 94
- F. Pin Assignment 96
  - VGA HD-15 96
  - RJ45 Connector Ethernet 96
- G. Specifications 97
  - Sizes and Weight 97
  - Environment 97
  - Temperature 97
  - Humidity 97
- H. B050-000 Operation Advices 98
- I. FCC Statement 98
- J. Tripp Lite Warranty Information 99
  - Limited Warranty 99
  - Warranty Registration 99

1. Quick Start Guide

Installation

The B050-000 redirects local keyboard, mouse and video data to a remote administration console. All data is transmitted with the TCP/IP protocol. The B050-000 can be used in a multi-administrator and multi-server environment. Combining the B050-000 with a KVM switch allows the user to access multiple remote servers over single remote console.

Connectors and Indicators

General Overview

The B050-000 has peripheral interfaces and indicators on both the front and rear side of the device. See the following sections for a detailed description of each side.

Figure 1-1. Connectors and Indicators (General Overview)

1. Quick Start Guide

Front Side Connectors (Figure 1-2)

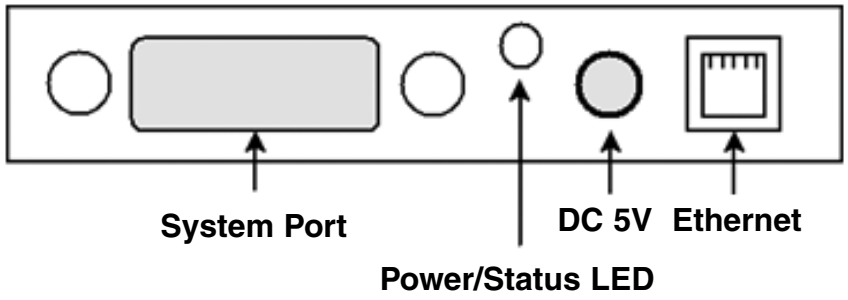


Figure 1-2. Front Side Connectors and Indicators

System Port:

- Attach the system cable with the gray connector to this port.

Power/Status LED:

- **LED off:** the B050-000 has no or not enough power
- **LED blinking:** the B050-000 is booting up (if this process takes longer than one minute, the reason may be a lack of power)
- **LED on:** the B050-000 is up and running

If the B050-000 is connected via USB-only and the Power/Status LED does not stop blinking after one minute, the B050-000 may not be receiving enough power via the USB port. You must then attach the enclosed power supply to the B050-000.

DC 5V (Power Supply):

- Attach the enclosed power supply to the B050-000
- Voltage: 5V
- Current: 1.5 A

RJ45 Ethernet:

- Cat5e UTP cables can be connected to the B050-000 using this standard RJ45 jack

1. Quick Start Guide

Rear Side Connectors (Figure 1-3)

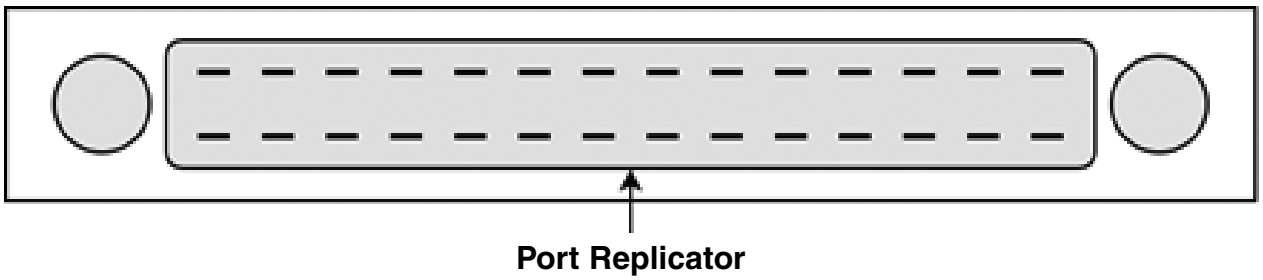


Figure 1-3. Rear Side Connectors

Port Replicator:

- Attach the port replicator cable here if you need PS/2 support

Connecting the B050-000 to the Host System

Perform the following steps in order to connect the KVM signals of the server system to the B050-000:

1. Attach the provided cables to
    - The VGA outlet on your server or the local console video port on your KVM Switch. Use the blue VGA connector
    - One of the USB ports on your server or your USB KVM switch or server
2. Connect the RJ45 Ethernet connector to your local Ethernet hub using a CAT5 or CAT6 Ethernet cable.
3. Connect the external power supply to the 5V power connector and power on the B050-000.

Warning: The USB standard guarantees up to 500mA power per single USB port. The B050-000 needs up to 700mA current and therefore is not guaranteed to work on USB alone. However, most of the current USB ports provide more than 700mA so that no external power is needed to power the B050-000. Taking more power from a USB port than specified may cause damage to your computer and therefore we recommend using the B050-000 AC adapter at all times.

1. Quick Start Guide

Initial Network Configuration

The B050-000 network interface is configured with the parameters shown in Table 1-1.

Parameter	Value
IP auto configuration	DHCP
IP address	—
Netmask	255.255.255.0
Gateway	none
IP access control	none

Table 1-1. Initial Network Configuration

Warning: If the DHCP connection fails on boot up, the B050-000 will not have an IP address.

If this initial configuration does not meet your local requirements, adjust the values as needed. You may either configure the B050-000 via serial interface or use the setup tool that can be found on the CD-ROM delivered with this package.

B050-000 Setup Tool

The setup tool is used to determine the IP address assigned to the B050-000 by the DHCP server or to change the device's initial network configuration.

Main Window

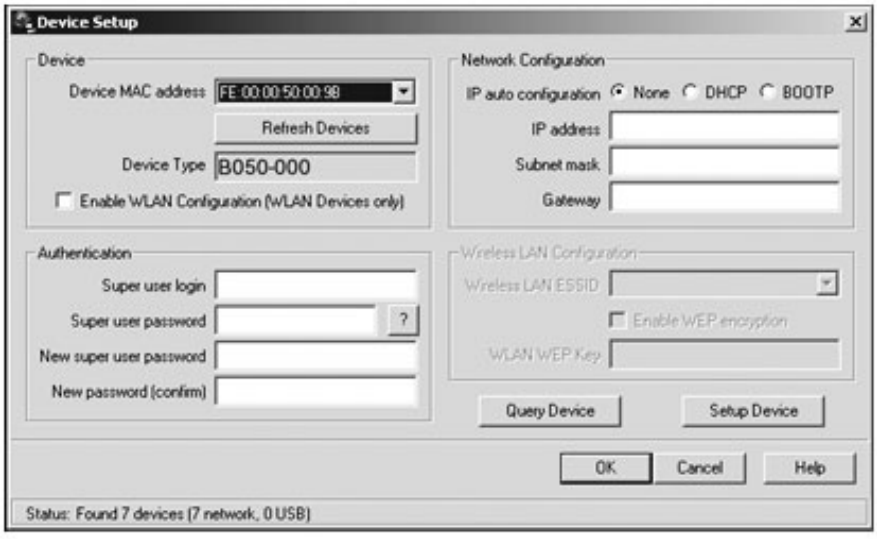


Figure 1-4. B050-000 Setup Tool (Windows Version)

1. Quick Start Guide

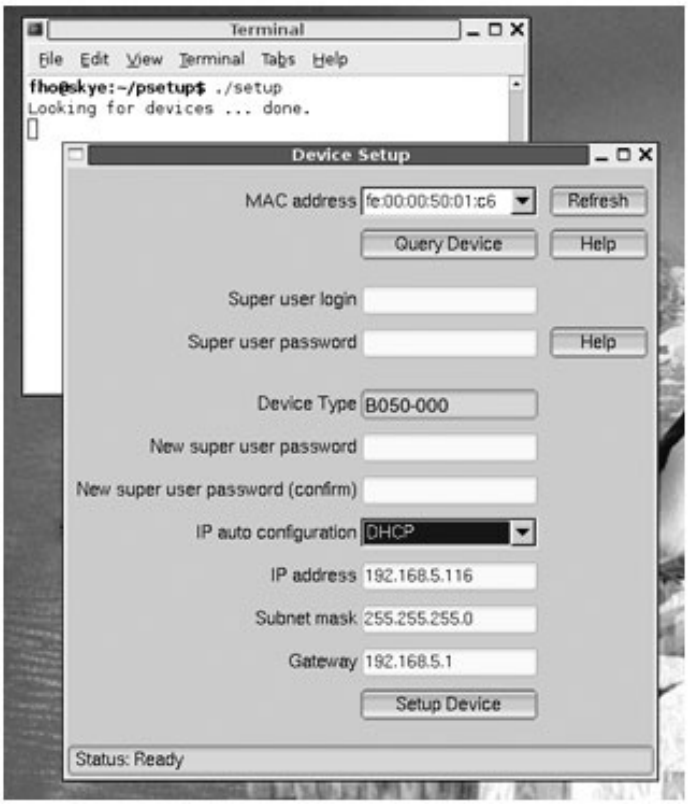


Figure 1-5. B050-000 Setup Tool (Linux Version)

Connect the B050-000 to your computer via local network or via USB. Start the setup tool from the CD-ROM on the computer where the B050-000 is installed. Depending on the connection (USB or network), the device detection is different.

> **Note:** Configuration via network requires the device to have a valid IP address. If your network provides a properly configured DHCP server, the B050-000 should be assigned an IP address automatically.

A window opens as seen in Figure 1-4 (Windows OS) or Figure 1-5 (Linux OS).

MAC Address Detection

Using the Windows Tool:

The MAC address of the B050-000 is displayed on the upper left corner of the screen. To detect the MAC address manually, press the “Refresh Devices” button. The displayed MAC address is the same MAC address printed on the white sticker placed on the back of the B050-000. If the B050-000 is connected via USB, it is classified as a USB device and an appropriate drive letter is chosen for this device. On the lower right corner of the window, there are two buttons: “Query Device” and “Setup Device”. Press the “Query Device” button to display the preconfigured values of the network configuration. The values are displayed in the “Network Configuration” text fields. If necessary, adjust the network settings to your needs. To save the changes enter a user name and password, then press the “Setup Device” button.

Using the Linux Tool:

The MAC address of the B050-000 is displayed on the upper left corner of the screen. To detect the MAC address manually, press the "Refresh" button. The displayed MAC address is the same MAC address printed on the white sticker placed on the back of the B050-000. The Linux setup tool currently does not support device configuration via the USB interface. Please use either a network connection or the serial console for the initial device configuration. Furthermore, there are two buttons on the window: "Query Device" and "Setup Device". Press the "Query Device" button to display the reconfigured values of the network configuration. The values are displayed in the text fields located nearby. If necessary, adjust the network settings to your needs. To save the changes enter a user name and password, then press the "Setup Device" button.

Authentication

To adjust the authentication settings, enter your login as a Super User and change your password.

Super User Login:

- Enter the login name of the super user. The initial value is "super".

Super User Password:

- Enter the current password for the super user. The initial value is "pass".

New Super User Password:

- Enter the new password for the Super User.

New Password (Confirm):

- Re-type the new password for the Super User. To close the window and accept the changes press the "OK" button, otherwise press the "Cancel" button (on Windows). On a Linux system, close the window by the appropriate button on the window frame.

Configuration via Serial Interface

To configure the B050-000 via serial interface, both a serial port replicator cable and a null modem cable are required (available separately). Connect the null modem cable to the serial interface with the black connector on the port replicator. The serial interface needs to be adjusted with the parameters as shown in Table 1-2.

Parameter	Value
Bits/second	115200
Data bits	8
Parity	no
Stop bits	1
Flow control	none

Table 1-2. Serial Parameters

1. Quick Start Guide

Use terminal software (e.g. hyperterm or minicom) to connect to the B050-000. Reset the B050-000, and immediately press the “ESC” key. You will see a “=>” prompt. Enter the command “config”, and press the “ENTER” key. You will be asked to adjust the IP auto configuration, the IP address, the net mask, and the default gateway. Pressing the “ENTER” key without entering values does not change settings. The gateway value has to be set to 0.0.0.0 (for no gateway) or any other value for the IP address of the gateway. After the confirmation, the B050-000 performs a reset using the new values.

Web Interface

The B050-000 may be accessed using a standard Java enabled web browser. You may use the HTTP protocol or a secure encrypted connection via HTTPS. Just enter the configured IP address of the B050-000 into your web browser. The initial login settings are:

Parameter	Value
Login	super
Password	pass

Table 1-3. Standard User Settings

Note: Changing these settings to user-specific values is strongly recommended and can be done on the “User Management” page (see the Section called “Users And Groups” in Chapter 6).

The Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system in which the B050-000 is installed. The web browser, which is used for accessing the B050-000, has to supply a Java Runtime Environment version 1.1 or higher. However, it is strongly recommended to install Sun JVM 1.4. The Remote Console will behave exactly the same way as if you were sitting directly in front of the screen of your remote system. That means that both the keyboard and mouse can be used in the usual way. Open the console by selecting the preview picture on the main site of the HTML front-end. Figure 1-6 shows the top of the Remote Console.

1. Quick Start Guide

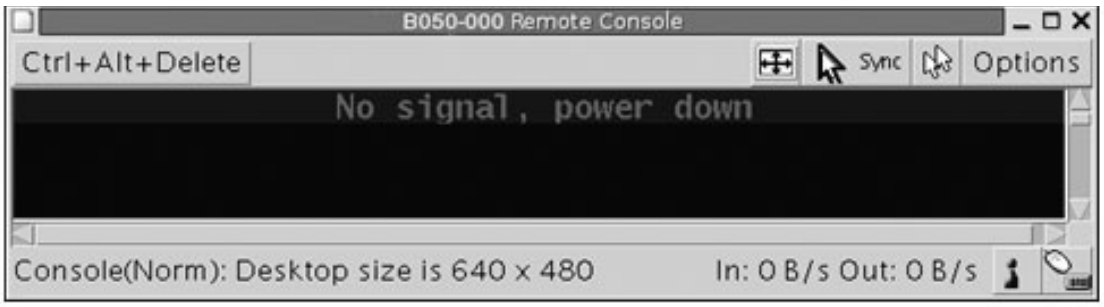
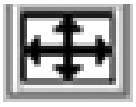


Figure 1-6. Top Part of the Remote Console

There are some menu options to choose from, the important ones are the following:



Auto Adjust Button

If the video displayed is of bad quality or distorted in some way, press this button and wait a few seconds while the B050-000 tries to adjust itself for the best possible video quality.

Sync Mouse

Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings.

Video Settings in Options Menu

This opens a new window with elements to control the B050-000 Video Settings. You can change some values such as brightness and contrast, which may improve the video quality. It is also possible to revert to the default settings for all video modes or only the current one.

> **Note:** At first start, if the local mouse pointer is not synchronized with the remote mouse pointer, press the Auto Adjust Button once.

2. Introduction

The B050-000 is a manufacturer-independent remote administration system. The B050-000 works as an integrated solution on your server system. Based on an embedded operating system, the B050-000 provides both exceptional stability and permanent availability independent of the present state of the server's operating system. As a system administrator, you have entire control and location-independent remote access to react upon both critical incidents and cases of necessary maintenance.

Figure 2-1. The B050-000

Features

The B050-000 defines a new class of remote access devices. It combines digital remote access via IP networks with comprehensive and integrated system management. The B050-000 offers convenient, remote KVM access and control via LAN or Internet. It captures, digitizes, and compresses video and transmits it with keyboard and mouse signals to and from a remote computer. Remote access and control software runs on its embedded processors only and not on mission critical servers, so that there is no interference with server operation or impact on network performance. Features of the B050-000 are:

- KVM (keyboard, video, mouse) access over IP or analog telephone line
- No impact on server or network performance
- Automatically senses video resolution for best possible screen capture
- High-performance mouse tracking and synchronization
- Port to connect a user console for direct analogous access to KVM device
- Local Mouse suppression (only when using a SUN Java Virtual Machine)

2. Introduction

B050-000 System Components

The B050-000 is a stand-alone product with the following dimensions: 3.75” (D) x 1” (H) x 73” (W)

The B050-000 is shipped with:

- A B050-000 base unit
- A external power supply
- A power cord
- A KVM cable
- Transparent equipment feet
- An Owner's Manual
- A Virtual Floppy Instructions Addendum
- A Quick Start Guide

When the Server is Up and Running

The B050-000 gives you full control over the remote server. The Management Console allows you to access the remote server’s graphics, keyboard and mouse and lets you send special commands to the server. You can also perform periodic maintenance of the server. Using the Console Redirection Service you can do the following:

- Reboot the system (a graceful shutdown)
- Watch the boot process
- Boot the system from a separate partition to load the diagnostic environment
- Run special diagnostic programs

When the Server is Dead

Fixing hardware defects is not possible using a remote management device. Nevertheless, the B050-000 gives the administrator valuable information about the type of hardware failure. Serious hardware failures can be organized into five different categories (According to a survey made by the Intel Corp.):

Category	Probability
Hard disk failure	50%
Power cable detached, power supply failure	28%
CPU, Controller, motherboard failure	10%
CPU fan failure	8%
RAM failure	4%

Table 2-1. Hardware Failures

2. Introduction

The B050-000 allows administrators to determine which kind of serious hardware failure has occurred (see Table 2-2).

Type of failure	Detected by
Hard disk failure	Console screen, CMOS set-up information
Power cable detached, power supply failure	Server remains in power off state after power on command has been given
CPU, Controller, main board failure	Power supply is on, but there is no video output
CPU fan failure	By IPMI or server specific management software
RAM failure	Boot-Sequence on boot console

Table 2-2. Host System Failures and How They are Detected

3. Installation

Operation Overview

The B050-000 redirects local keyboard, mouse and video data to a remote administration console. All data is transmitted with the TCP/IP protocol.

The B050-000 can be used in both a multi-administrator and multi-server environment. Combining one or more B050-000 with a single KVM switch allows access to multiple servers on a single remote console.

Connectors and Indicators

General Overview

The B050-000 has peripheral interfaces and indicators on the front and rear ends of the device. See the following sections for a detailed description of each side.

Figure 3-1. Connectors and Indicators (General Overview)

3. Installation

Front Connectors and Indicators

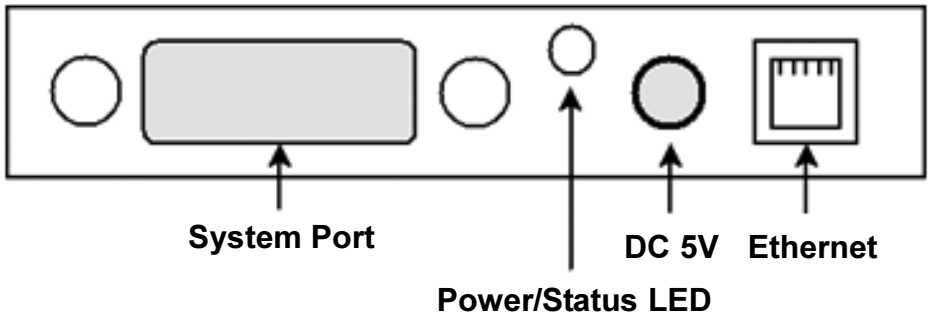


Figure 3-2. Front Connectors and Indicators

System Port:
Attach the system cable with the gray connector to this port.

Power/Status LED:

- **LED off:** the B050-000 has no or not enough power
- **LED blinking:** the B050-000 is booting up (if this process takes longer than one minute, the reason may be a lack of power)
- **LED on:** the B050-000 is up and running

If the B050-000 is connected via USB-only and the Power/Status LED does not stop blinking after one minute, the B050-000 may not be receiving enough power via the USB port. In that case attach the enclosed power supply to the B050-000.

DC 5V (Power Supply):

- Attach the enclosed power supply to the B050-000
- **Voltage:** 5V
- **Current:** 1.5 A

RJ45 Ethernet:

- Cat5 UTP cables can be connected to the B050-000 using this standard RJ45 jack

3. Installation

Rear Side Connectors

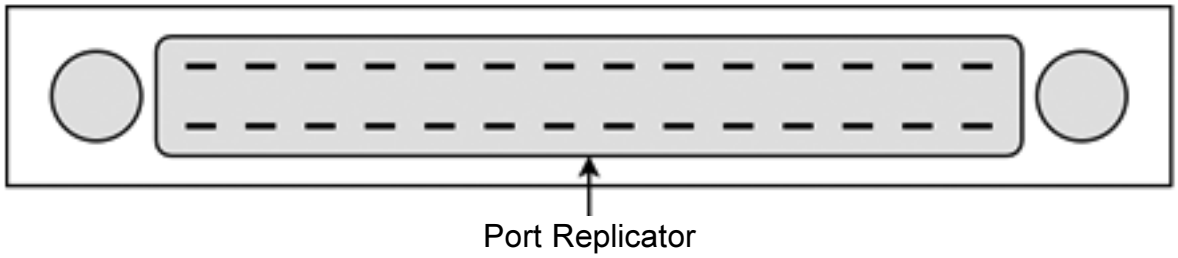


Figure 3-3. Rear Side Connectors

Port Replicator:

- Attach the port replicator cable to enable PS/2 support

Connecting the B050-000 to the Host System

To connect the server to the B050-000:

1. Attach the provided cable(s) to:
   - The VGA outlet on your server or the local console video port on your KVM Switch. Use the blue VGA connector
   - Either the USB port on your server or your KVM Switch (or the PS/2 connector on the alternate cable to the PS/2 ports on your server or KVM)
2. Connect the RJ45 Ethernet connector to your local Ethernet hub using a CAT5 or CAT6 Ethernet cable.
3. Connect the external power supply to the 5V power connector and power on the B050-000.

Warning: The USB standard guarantees up to 500mA of power per single USB port. The B050-000 needs up to 700mA current and therefore is not guaranteed to work on USB alone. However, most of the current USB ports provide more than 700mA so that no external power is needed to power the B050-000. Taking more power from a USB port than specified may cause damage to your computer and therefore we recommend using the B050-000 AC adapter at all times.

3. Installation

Connecting a Local Console

To connect a local console to the host system besides the B050-000 you may attach a monitor, a keyboard and a mouse to the connectors on the port replicator (available separately).

Connecting Ethernet

On the front of the B050-000 is an RJ45 connector for Ethernet. The connector is used either for a 100 Mbps 100Base-TX connection or for a 10 Mbps 10BASE-T connection. The adapter can sense the connection speed and will adjust to the appropriate operation mode automatically.

10 Mbps Connection

For 10BASE-T Ethernet networks, use category 5 UTP cable. To establish a 10 Mbps connection, the cable has to be connected to a 10BASE-T hub.

1. Make sure that the cable is wired appropriately for a standard 10BASE-T Adapter (use Tripp Lite N001, N002 or N201 series cables).
2. Insert the cable into the RJ45 connector on the adapter.

100 Mbps Connection

For 100BASE-TX Ethernet networks, the B050-000 supports category 5 UTP cabling. To establish a 100 Mbps connection, the cable has to be connected to a 100BASE-TX hub.

1. Make sure that the cable is wired appropriately for a standard 10BASE-T Adapter (use Tripp Lite N001, N002 or N201 series cables).
2. Insert the cable into the RJ45 connector on the adapter.

Warning: The UTP wire pairs and configuration for 100BASE-TX cable are identical to those for 10BASE-T cable when used with category 5 UTP cable.

4. Configuration

Initial Configuration

The B050-000's communication interfaces are all based on TCP/IP. It comes preconfigured with the IP configuration listed in Table 4-1.

Parameter	Value
IP auto configuration	DHCP
IP address	—
Netmask	255.255.255.0
Gateway	none
IP access control	none

Table 4-1. Initial Network Configuration

Warning: If the DHCP connection fails on boot up, the B050-000 will not have an IP address.

If this initial configuration does not meet your requirements, the following describes the initial IP configuration that is necessary to access the B050-000 for the first time.

B050-000 Setup Tool

The setup tool is used to determine the IP address assigned to the B050-000 by the DHCP server or to change the device's initial network configuration.

Main Window

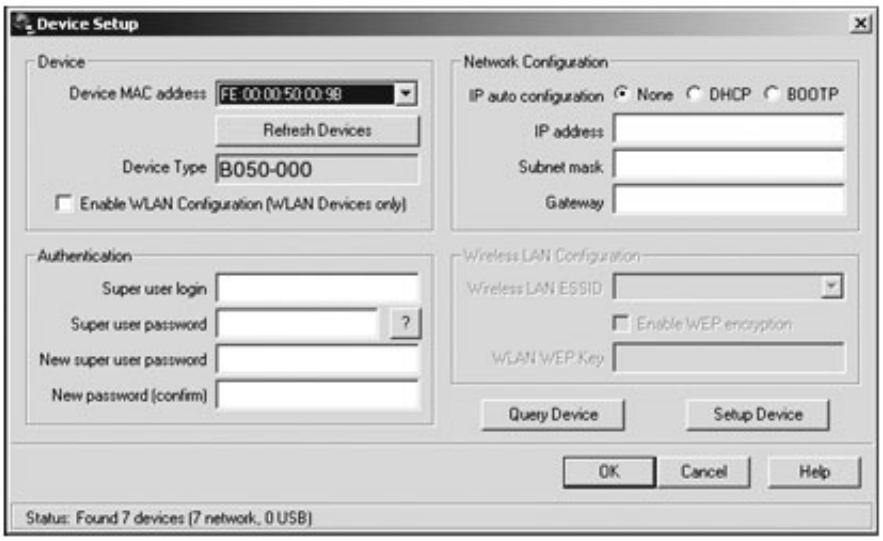


Figure 4-1. B050-000 Setup Tool (Windows Version)

4. Configuration

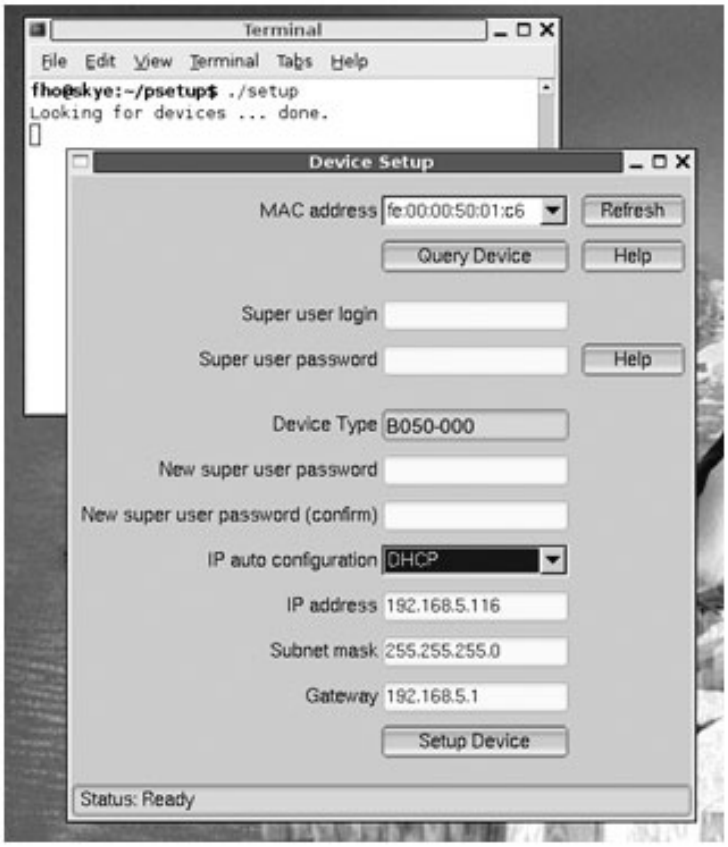


Figure 4-2. B050-000 Setup Tool (Linux Version)

Connect the B050-000 to your computer either via the local network or via the USB port. Start the setup tool from the CD-ROM on the computer that is connected to the B050-000. The device detection depends on the type of connection (USB or network).

> **Note:** Configuration via a network requires the device to have a valid IP address. If your network provides a properly configured DHCP server, the B050-000 should be assigned an IP address automatically.

A window opens as seen in Figure 4-1 (Windows OS) and Figure 4-2 (Linux OS).

MAC Address Detection

Using the Tool for Windows

The MAC address of the B050-000 is displayed on the upper left hand corner of the screen. To detect the MAC address manually, press the “Refresh Devices” button. The displayed MAC address is the same MAC address printed on the white sticker placed on the back of the B050-000. If the B050-000 is connected via USB, it is classified as a USB device and an appropriate drive letter is chosen for this device. On the lower right corner of the window, there are two buttons: “Query Device” and “Setup Device”. Press the “Query Device” button to display the preconfigured values of the network configuration. The values are displayed in the “Network Configuration” text fields. If necessary, adjust the network settings to your needs. To save the changes enter a user name and password, then press the “Setup Device” button.

4. Configuration

Using the Linux Tool:

The MAC address of the B050-000 is displayed on the upper left corner of the screen. To detect the MAC address manually, press the “Refresh” button. The displayed MAC address is the same MAC address printed on the white sticker placed on the back of the B050-000. The Linux setup tool currently does not support device configuration via the USB interface. Please use either a network connection or the serial console for the initial device configuration. Furthermore, there are two buttons on the window: “Query Device” and “Setup Device”. Press the “Query Device” button to display the reconfigured values of the network configuration. The values are displayed in the text fields located nearby. If necessary, adjust the network settings to your needs. To save the changes enter a user name and password, then press the “Setup Device” button.

Authentication

To adjust the authentication settings, enter your login as a Super User and change your password.

Super User Login:
- Enter the login name of the Super User. The initial value is “super”.

Super User Password:
- Enter the current password for the super user. The initial value is “pass”.

New Super User Password:
- Enter the new password for the Super User.

New Password (Confirm):
- Re-type the new password for the Super User. Press the “OK” button to close the window and accept the changes. Otherwise press the “Cancel” button (on Windows). On a Linux system close the window using the appropriate button on the window frame.

Initial Configuration via DHCP Server

By default, the B050-000 will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it may provide a valid IP address, gateway address and net mask. Before you connect the device to your local subnet, be sure to complete the corresponding configuration of your DHCP server. It is recommended to configure a fixed IP assignment to the MAC address of the B050-000. You can find the MAC address on the outside of the shipping box and labeled on the bottom side. If this initial configuration does not meet your local requirements, use the setup tool to adjust the values to your needs. The setup tool can be found on the CD ROM delivered with this package. You can follow the procedure described below.

4. Configuration

Initial Configuration via Serial Console

To configure the B050-000 via serial interface, both a serial port replicator cable and a null modem cable are required (available separately). Using a serial terminal, the B050-000 has a serial line interface (on the rear). This connector is compliant with the RS 232 serial line standard. To establish a serial connection, use a standard null modem cable. The serial line has to be configured with the parameters given in Table 4-2. When configuring with a serial terminal, reset the B050-000 and immediately press the "ESC" key. You will see a "=>" prompt. Enter "config", press "Enter" and wait for a few seconds for the configuration questions to appear.

Parameter	Value
Bits/second	115200
Data bits	8
Parity	no
Stop bits	1
Flow control	none

Table 4-2. Serial Line Parameters

As you proceed, the following questions will appear on the screen. To accept the default values, which are shown in square brackets below, press "Enter".

IP auto configuration (non/dhcp/bootp) [dhcp]:

IP [192.168.1.22]:

Net mask [255.255.255.0]:

Gateway (0.0.0.0 for none) [0.0.0.0]:

Web Interface

IP Autoconfiguration:

With this option you can specify whether the B050-000 should get its network settings from a DHCP or BOOTP server. For DHCP, enter "dhcp", and for BOOTP enter "bootp". If you do not specify any of these, the IP autoconfiguration is disabled and subsequently you will be asked for the following network settings.

IP Address:

The IP address the B050-000 uses. This option is only available if IP autoconfiguration is disabled.

Net Mask:

The net mask of the connected IP subnet. This option is only available if IP auto- configuration is disabled.

Gateway Address:

The IP address of the default router for the connected IP subnet. If you do not have a default router, enter 0.0.0.0. This option is only available if IP autoconfiguration is disabled.

Finally, you will be asked if the values are correct, and may adjust them if necessary. After your confirmation, the B050-000 performs a reset using the new values.

Parameter	Value
Login	super
Password	pass

Table 4-3. Standard User Settings

Note: Changing these settings to user specific values is strongly recommended and can be done on the "User Management" page (see the Section called Users And Groups in Chapter 6).

Mouse, Keyboard and Video Configuration

There are two interfaces available for transmitting keyboard and mouse data between the B050-000 and the host: USB and PS/2 (available separately). The correct operation of the remote mouse depends on several settings, which will be discussed in the following subsections.

B050-000 USB Interface

To use the USB interface, correct cabling between the managed host and the managing device is necessary. If the managed host does not have USB keyboard support in the BIOS and you have connected the USB cable only, then you will not have any remote keyboard access during the boot process of the host. Please see the Section called "Keyboard/Mouse" in Chapter 6 for more details.

B050-000 Keyboard Settings

The B050-000 settings for the host's keyboard type have to be correct in order to make the remote keyboard work properly. Check the settings in the B050-000 front-end. See the Section called Keyboard/Mouse in Chapter 6 or details.

Remote Mouse Settings

A common problem with KVM devices is the synchronization between the local and remote mouse cursors. The B050-000 addresses this situation with an intelligent synchronization algorithm. There are three mouse modes available on the B050-000.

Auto Mouse Speed

The automatic mouse speed mode tries to detect the speed and acceleration settings of the host system automatically. See the section below for a more detailed explanation.

Fixed Mouse Speed

This mode translates the mouse movements from the Remote Console in a way that one pixel move will lead to *n* pixel moves on the remote system. This parameter n is adjustable via scaling. It should be noted that this works only when mouse acceleration is turned off on the remote system.

Single/Double Mouse Mode

This mode is described in the Section called Single and Double Mouse Mode.

Auto Mouse Speed and Mouse Synchronization

The automatic mouse speed mode performs the speed detection during mouse synchronization. Whenever the mouse does not move correctly, there are two ways to re-synchronize the local and remote mouse:

Fast Sync:

Fast synchronization is used to correct a temporary but fixed skew. Choose this option from the Remote Console Options menu (entry: Mouse Handling). If defined, you may also press the mouse synchronization hotkey sequence (see the Section called Remote Console Control Bar in Chapter 5 for details).

Intelligent Sync:

If the Fast Sync does not work or the mouse settings have been changed on the host system, use the Intelligent Synchronization instead. This method adjusts the parameters for the actual movement of the mouse pointer so that the mouse pointer is displayed at the correct position on the screen. This method takes more time than the Fast Sync and can be accessed with the appropriate item in the Remote Console Option menu (entry: Mouse Handling). The Intelligent Synchronization requires a correctly adjusted picture. Use the Auto Adjustment function or the manual correction in the Video Settings panel to setup the picture. In addition, the shape of the mouse pointer has a significant influence on the pointer detection. We recommend using a simple, but common pointer shape. In most cases, the detection and synchronization of animated pointer shapes is likely to fail. In general, pointer shapes that change during the pointer detection process are hard to figure out in the transferred video picture. With the usage of a standard mouse pointer shape, the detection is much simpler and the synchronization is at its best.

Figure 4-3. Remote Console Control Bar: Sync Button

The behavior of the Sync Mouse button on top of the Remote Console depends on the current state of mouse synchronization. Pressing this button usually leads to a Fast Sync, except in situations where the video mode has been changed recently. See also the Section called Remote Console Control Bar in Chapter 5.

> **Note:** At first start, if the local mouse pointer is not synchronized with the remote mouse pointer, press the Auto Adjust Button once.

4. Configuration

Host System Mouse Settings

The host's operating system knows various settings for the mouse driver.

> **Warning: The following limitations do not apply in case of USB and Mouse Type "MS Windows 2000 and newer".**

While the B050-000 works with accelerated mice and is able to synchronize the local with the remote mouse pointer, the following limitations may prevent this synchronization from working properly:

Special Mouse Driver:

There are mouse drivers, which influence the synchronization process and lead to desynchronized mouse pointers. If this happens, make sure you do not use a special vendor-specific mouse driver on your host system.

Windows 2003 Server/XP Mouse Settings:

Windows XP knows a setting named "improve mouse acceleration" which has to be deactivated.

Active Desktop:

If the Active Desktop feature of Microsoft Windows is enabled, do not use a plain background. Instead, use some kind of wallpaper. As an alternative, you could also disable the Active Desktop completely.

Also see the Section titled Recommended Mouse Settings for mouse mode recommendations.

Navigate your mouse pointer into the upper left corner of the applet screen and move it slightly forth and back. The mouse will be resynchronized. If resynchronizing fails, disable the mouse acceleration and repeat the procedure.

Single and Double Mouse Mode

The information above applies to the Double Mouse Mode where remote and local mouse pointers are visible and need to be synchronized. The B050-000 also features another mode, the Single Mouse Mode, where only the remote mouse pointer is visible. Activate this mode in the Remote Console (see the Section called Remote Console Control Bar in Chapter 5) and click into the window area. The local mouse pointer will be hidden and the remote one can be controlled directly. To leave this mode it is necessary to define a mouse hotkey in the Remote Console Settings Panel. Press this key to free the captured local mouse pointer.

Recommended Mouse Settings

We suggest the following for the different operating systems:

MS Windows NT4:

NT4 supports PS/2 only. Please choose the options PS/2 mouse and Auto Mouse Speed.

MS Windows 2000, 2003, XP (all versions):

In general, we recommend using a mouse via USB. Choose USB without Mouse Sync. For a PS/2 mouse choose Auto Mouse Speed. For XP disable the option “enhance pointer precision” in the Control Panel.

Note: The remote mouse is always synchronized with the local mouse if selecting the option “MS Windows 2000 or newer”.

SUN Solaris:

Adjust the mouse settings either via “xset m 1” or use the CDE Control Panel to set the mouse to “1:1, no acceleration”. As an alternative you may also use the Single Mouse Mode.

MAC OS X:

We recommend using the Single Mouse Mode.

OS/2:

We recommend using the Single Mouse Mode.

Linux:

First, choose the option “Other Operating Systems” from the Mouse Type selection box. Then, choose the option Auto Mouse Speed. This applies for both USB and PS/2 mice.

Video Modes

The information above applies to the Double Mouse Mode where remote and local mouse pointers are visible and need to be synchronized. The B050-000 also features another mode, the Single Mouse Mode, where only the remote mouse pointer is visible. Activate this mode in the Remote Console (see the Section called Remote Console Control Bar in Chapter 5) and click into the window area. The local mouse pointer will be hidden and the remote one can be controlled directly. To leave this mode it is necessary to define a mouse hotkey in the Remote Console Settings Panel. Press this key to free the captured local mouse pointer.

Resetting the B050-000 to its Factory Settings

Using the Serial Interface

Reset the B050-000 and immediately press the “ESC” key. On your screen a command prompt “=>” will be visible. Enter the command “defaults”, press the “Enter” key and wait for a few seconds for the B050-000 to reboot. Now, you may use the default settings as described in the Section called Initial Configuration.

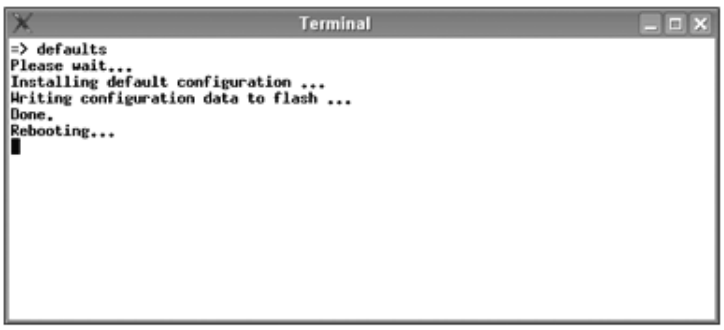


Figure 4-4. Terminal with Reset Messages

5. Usage

Prerequisites

The B050-000 features an embedded operating system and applications offering a variety of standardized interfaces. This chapter will describe both these interfaces and the way to use them in a more detailed manner. The interfaces are accessed using the TCP/IP protocol, thus they can be accessed using the built-in Ethernet adapter.

The following interfaces are supported:

HTTP/HTTPS:

Full access is provided by the embedded web server. The B050-000 environment can be entirely managed using a standard web browser. You can access the B050-000 using the unsecured HTTP protocol or using the encrypted HTTPS protocol. Whenever possible, use HTTPS.

Telnet:

A standard Telnet client can be used to access an arbitrary device connected to the B050-000's serial port via a terminal mode.

SSH:

The B050-000 also offers SSH (Secure Shell) access as a secure alternative to Telnet.

The primary interface of the B050-000 is the HTTP interface. This is covered extensively in this chapter. Other interfaces are addressed in subtopics. In order to use the Remote Console window of your managed host system, the browser has to come with a Java Runtime Environment version 1.1 or higher. If the browser does not have any Java support (such as on a small handheld device), you are still able to maintain your remote host system using the administration forms displayed by the browser itself.

Note: We recommend you install Sun JVM 1.4.

For an unsecured connection to the B050-000 we can recommend the following web browsers:

- Microsoft Internet Explorer version 5.0 or higher on Windows 98, Windows ME, Windows 2000 and Windows XP
- Netscape Navigator 7.0, Mozilla 1.6 and Mozilla Firefox on Windows 98, Windows ME, Windows 2000, Windows XP, Linux and other UNIX-like Operating Systems

In order to access the remote host system using a securely encrypted connection, you need a browser that supports the HTTPS protocol. Strong security is only assured by using a key length of 128 Bit. Some of the old browsers do not have a strong 128 Bit encryption algorithm. Using the Internet Explorer, open the menu entry “?” and “Info” to read about the key length that is currently activated.

5. Usage

A link will lead you to information on how to upgrade your browser to a state of the art encryption scheme. Figure 5-1 shows the dialog box presented by the Internet Explorer 6.0.

Figure 5-1. The Internet Explorer Displaying the Encryption Key Length

Note: Newer web browsers do support strong encryption by default.

Login to the B050-000 and Logout

Login to the B050-000

Open your web browser. Type in the address of the B050-000 you configured during the installation process. The address used might be a plain IP address or a host and domain name (in case you have given your B050-000 a symbolic name in the DNS). For instance, type the following in the address line of your browser when establishing an unsecured connection:

http://192.168.1.22/

In order to use a secure connection type in:

https://192.168.1.22/

This will lead you to the B050-000 login page as shown in Figure 5-2.

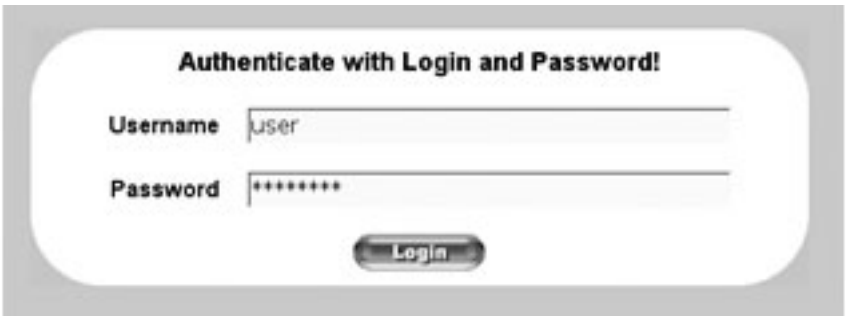


Figure 5-2. Login Screen

5. Usage

Warning: Your web browser has to accept cookies or else login is not possible.

The B050-000 has a built-in Super User that has all the permissions to administrate your B050-000. See the following table for the default settings. Please note that the user “super” is not allowed to login via the serial interface of the B050-000.

Parameter	Value
Login	super
Password	pass

Table 5-1. Standard User Settings

Warning: Please make sure to change the super user password immediately after you have installed and accessed your B050-000 for the first time. Not changing the pass phrase for the super user is a severe security risk and might result in unauthorized access to the B050-000 and to the host system including all possible consequences!

Navigation

Once you’ve logged into the B050-000 successfully, the main page of the B050-000 appears (see Figure 5-3). This page consists of three parts, each of which contains specific information. The buttons on the upper side allow you to navigate within the front end (see Table 5-2 for details). The lower left frame contains a navigation bar and allows you to switch between the different sections of the B050-000. In the right frame, task-specific information is displayed based on the section you have chosen before.

5. Usage

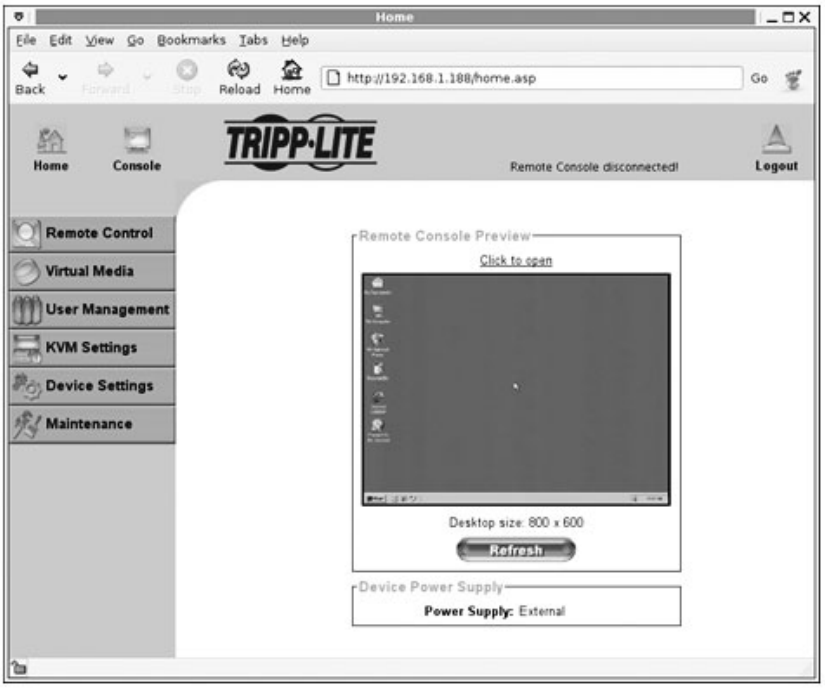


Figure 5-3. Main Page

Return to the main page of the B050-000.

Open the B050-000 Remote Console.

Exit from the B050-000 front end.

Table 5-2. Buttons from the Front End

Warning: If there is no activity for half an hour, the B050-000 will log you out automatically. A click on one of the links will bring you back to the login screen.

Logout from the B050-000

This link logs out the current user and opens a new login screen. Please note that an automatic logout will be performed if there isn't any activity for half an hour.

5. Usage

The Remote Console

General Description

The Remote Console is the redirected screen, keyboard and mouse of the remote host system that the B050-000 controls.

Figure 5-4. Remote Console

The Remote Console window is a Java Applet that tries to establish its own TCP connection to the B050-000. The protocol that is run over this connection is neither HTTP nor HTTPS, but RFB (Remote Frame Buffer Protocol). Currently RFB tries to establish a connection to port #443. Your local network environment has to allow this connection to be made, i.e. your firewall and, in case you have a private internal network, your NAT (Network Address Translation) settings have to be configured accordingly.

In case the B050-000 is connected to your local network environment and your connection to the Internet is available using a proxy server only without NAT being configured, the Remote Console is very unlikely to be able to establish the appropriate connection. The reason is that today's web proxies are not capable of relaying the RFB protocol. In case of problems, please consult your network administrator in order to provide an appropriate network environment.

Main Window

Starting the Remote Console opens an new window. It displays the screen content of your host system. The Remote Console will behave exactly in the same way as if you were sitting directly in front of the screen of your remote system. That means keyboard and mouse can be used in the usual way. However, be aware that the remote system will react to keyboard and mouse actions with a slight delay. The delay depends on the bandwidth of the line, which you use to connect to the B050-000.

5. Usage

With respect to the keyboard, there may be some confusion if the remote and local keyboards have different keyboard layouts. Your local keyboard changes its keyboard layout in accordance with the remote host system. For instance, if you use a Spanish administration system and your host system uses a US English keyboard layout, special keys on the Spanish keyboard will not work as expected. Instead, the keys will result in their US English counterpart. You can circumvent such problems by adjusting the keyboard of your remote system to the same mapping as your local one. The Remote Console window always tries to show the remote screen with its optimal size. That means it will adapt its size to the size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, you can always resize the Remote Console window in your local window system as usual.

Warning: The Remote Console window on your local window system is just one window among others. In order to make keyboard and mouse work, your Remote Console window must have the local input focus.

Remote Console Control Bar

The upper part of the Remote Console window contains a control bar. Using its elements you can see the status of the Remote Console and influence the local Remote Console settings. A description for each control follows.

Figure 5-5. Remote Console Control Bar

Ctrl+Alt+Delete
Special button key used to send the "Control Alt Delete" key combination to the remote system (see also the Section called KVM Settings in Chapter 6 for defining new button keys).

Auto Adjust Button
If the video displayed is of bad quality or distorted in some way, press this button and wait a few seconds while the B050-000 tries to adjust itself for the best possible video quality.

Sync Mouse
Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general, there is not a need to change mouse settings on that system.

5. Usage

Single/Double Mouse Mode
Switches between the Single Mouse Mode (where only the remote mouse pointer is visible) and the Double Mouse Mode (where remote and local mouse pointers are visible and need to be synchronized). Single Mouse Mode is only available if using SUN JVM 1.4 or higher.

Options
To open the Options menu, click on the button “Options”. See the Section called Remote Console Options for a detailed description of the available options for the B050-000.

Remote Console Options

To open the Options menu click on the button “Options”.

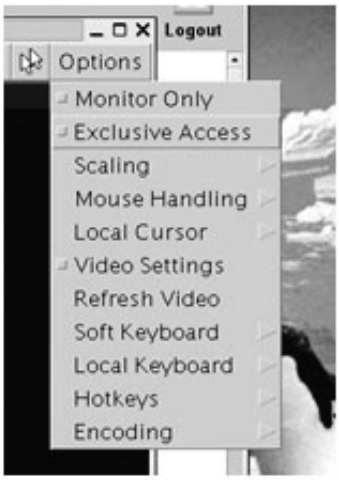


Figure 5-6. Remote Console Options Menu

A description of the options follows.

Monitor Only:
Toggles the Monitor Only filter on or off. If the filter is switched to on, no remote console interaction is possible. The remote screen can be viewed, only.

Exclusive Access:
If a user has the appropriate permission, he can force the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access or logs off.

Note: This option is only accessible for members of the “administrator” group and the user “super”.

A change in the access mode is also visible in the status line. See the Section called “Remote Console Status Line” for more information.

Scaling:

Allows you to scale down the Remote Console. You can still use the mouse and keyboard, however the scaling algorithm will not preserve all display details.

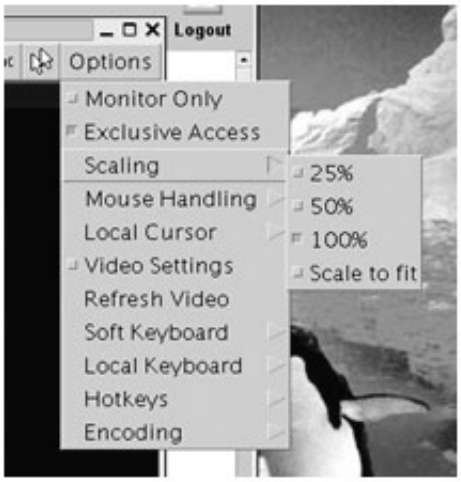


Figure 5-7. Remote Console Options Menu: Scaling

Mouse Handling:

The submenu for mouse handling offers two options for synchronizing the local and remote mouse pointer as explained in the Section called Mouse, Keyboard and Video Configuration in Chapter 4.

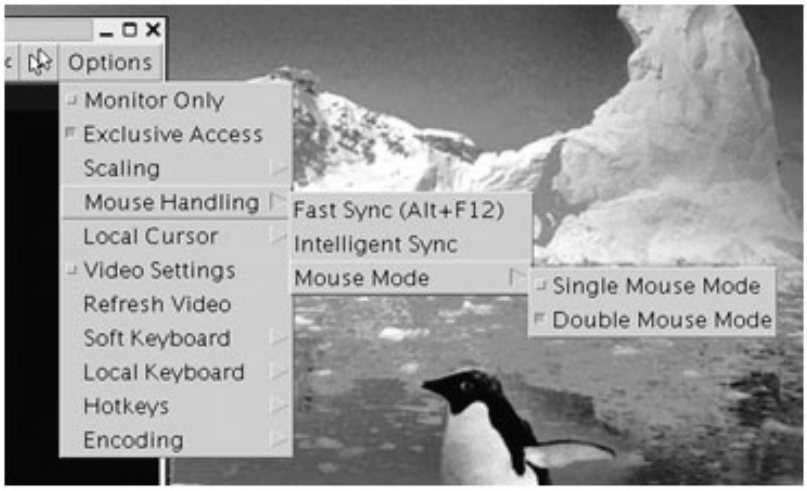


Figure 5-8. Remote Console Options Menu: Mouse Handling

- **Fast Sync**

  The fast synchronization is used to correct a temporary but fixed skew.

- **Intelligent Sync**

  Use this option if the fast sync does not work or the mouse settings have been changed on the host system.

5. Usage

Warning: Intelligent Sync takes more time than Fast Sync and requires a correctly adjusted picture. To set up the picture you may use either the auto adjustment function or the manual correction in the Video Settings panel.

Local Cursor:

Offers a list of different cursor shapes to choose from for the local mouse pointer. The selected shape will be saved for the current user and activated the next time this user opens the Remote Console. The number of available shapes depends on the Java Virtual Machine, a version of 1.2 or higher offers the full list.

Figure 5-9. Remote Console Options Menu: Cursor

Video Settings:

Opens a panel used to change the B050-000 video settings. The B050-000 features two different dialogs which influence the video settings.

Video Settings through the HTML Front End:

Select this option to enable the local video port. This option decides if the local video output of the B050-000 is active and passing through the incoming signal from the host system.

The option Noise Filter defines how the B050-000 reacts to small changes in the video input signal. A large filter setting needs less network traffic and leads to a faster video display but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if display content is not really changing (depending on the quality of the video input signal). All in all, the default setting should be suitable for most situations.

5. Usage

Video Settings through the remote console

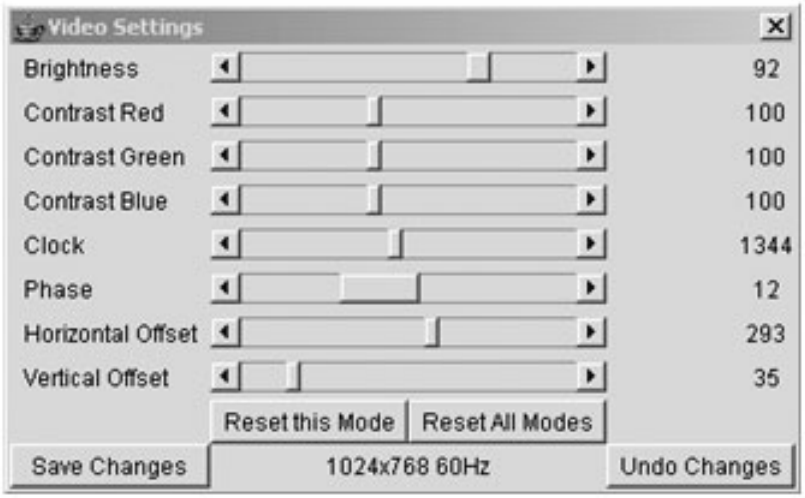


Figure 5-10. Video Settings Panel

Brightness:
Controls the brightness of the picture.

Contrast:
Controls the contrast of the picture.

Clock:
Defines the horizontal frequency for a video line and depends on the video mode. Different video card types may require different values. The default settings in conjunction with the auto adjustment procedure should be adequate for all common configurations. To achieve a better picture quality you may try to change this setting together with the sampling phase.

Phase:
Defines the phase for video sampling, used to control the display quality together with the setting for sampling clock.

Horizontal Position:
Use the left and right buttons to move the picture in a horizontal direction while this option is selected.

Vertical Position:
Use the left and right buttons to move the picture in a vertical direction while this option is selected.

Reset this Mode:
Reset mode specific settings to the factory-defined defaults.

Reset all Modes:
Reset all settings to the factory-defined defaults.

Save Changes:
Save changes permanently.

Undo Changes:

Restore last settings.

Note: The Video Settings Panel and the according entry in the Options menu are only available for members of the “administrator” group and the user “super”.

Refresh Video:

Use this option to refresh the video picture. The video data for the Remote Console is updated completely. On startup of the Remote Console, the B050-000 transmits the entire video picture from the remote host. Subsequently, the parts of the video picture that did not change are filtered and not transmitted again. This leads to less video data to be transmitted. It may happen that there are parts of the video picture that are not updated correctly (video noise, compression errors). You may use this option to initiate an entire refresh, manually.

Soft Keyboard:

The Soft Keyboard simulates an entire keyboard that is connected to the remote system. It is necessary in case your remote system runs with a completely different language and country mapping than your administration machine. By selecting the according button(s) you can send key codes and also key sequences to the remote system and act as if you would work with a keyboard that is directly connected to the remote system.

In order to open the Soft Keyboard, select the entry “Soft Keyboard” from the Options menu. You can send single key strokes like F as well as combinations of keys such as Ctrl+C or AltGr+Shift+F4.
For a single key stroke you can click on the button with the desired character. Single keys such as regular characters and numbers are sent immediately. Special keys like Ctrl, Shift as well as the function keys F1 to F12 have to be selected twice. The first press sends the signal “key is pressed”, the second press indicated the signal “key is released” to the remote system. After the first press the button will change its color to signalize that the associated key is pressed, currently. After the second press the button will appear as usual and signalize that the key was sent. To send the key combination Ctrl+C select the button Ctrl first. The button will change its color. Press the button C. The following key (C in our example) will be combined with the previously selected key. Both the buttons Ctrl and C are released and the key combination will be sent to the remote system. The button Ctrl will appear as normal (color change).

In order to send the key combination Ctrl+F5 three steps have to be done. Select the button Ctrl once and the button F5 twice. The last press will release both buttons and send the key combination to the remote system. In order to send the key combination AltGr+Shift+F4 four steps are required. First, select the button AltGr once. Second, select the button Shift. Finally, choose the button F4 twice. The last press will release all the buttons and send the key combination to the remote system.

Figure 5-11. Soft Keyboard

- **Show**
  Displays the Soft Keyboard.

- **Mapping**
  Used for choosing the according language and country mapping of the Soft Keyboard.

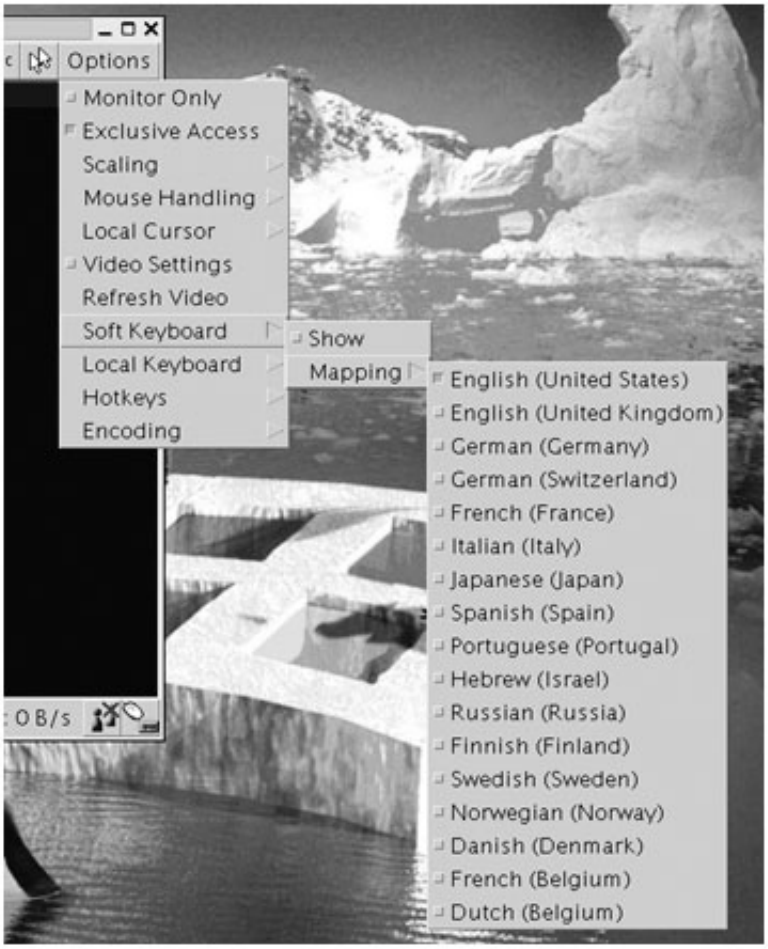


Figure 5-12. Soft Keyboard Mapping

Local Keyboard:

Used to change the language mapping of your browser machine running the Remote Console Applet. Normally, the applet determines the correct value automatically. However, depending on your particular JVM and your browser settings this is not always possible. A typical example is a Spanish localized system that uses a US-English keyboard mapping. In this case you have to change the Local Keyboard setting to the right l anguage manually.

Hotkeys:

Opens a list of hotkeys previously defined. In order to send a registered command to the host system, choose the appropriate entry. A confirmation dialog can be added that will be displayed before sending the selected command to the remote host. Choose "OK" to perform the command on the remote host. For a detailed description see the Section called Remote Console Button Keys in Chapter 6.

Figure 5-13. Remote Console Confirmation Dialog

Encoding:

These options are used to adjust the encoding level in terms of compression and color depth. They are only available if the "Transmission Encoding" is not determined automatically (see the Section called Transmission Encoding in Chapter 6).

- **Compression level**
  You may select a value between 1 and 9 for the desired compression level with level 1 enabling the fastest compression and level 9 the best compression. The most suitable compression level should always be seen as a compromise between the network bandwidth that is available on your video picture to be transferred, and on the number of changes between two single video pictures. We recommend using a higher compression level if the network bandwidth is low. The higher the compression level, the more time is necessary to both pack or unpack the video data on either side of the connection. The compression quality depends on the video picture itself, e.g. the number of the colors or the diversity of pixels. The lower the compression quality, the more data have to be sent and the longer it may take to transfer the whole video picture. If level 0 is chosen the video compression is disabled, completely. The option "Video Optimized" has its advantages if transferring high-quality motion pictures. In this case the video compression is disabled, completely and all video data is transferred via network as full-quality video snippets. Therefore, a high amount of bandwidth is required to ensure the quality of the video picture.

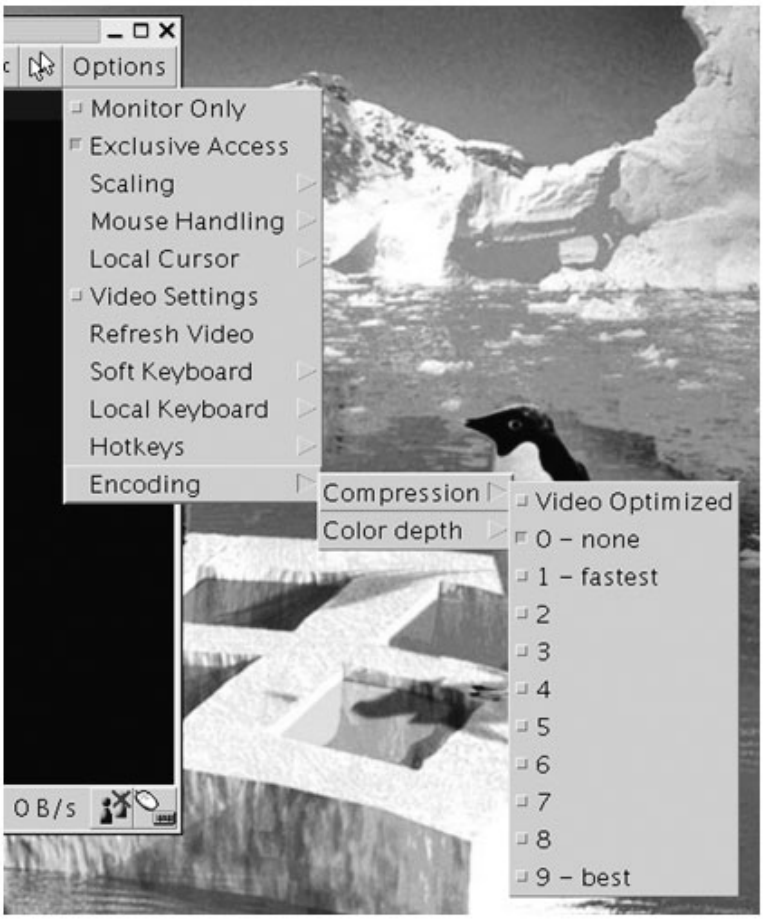


Figure 5-14. Remote Console Options: Encoding Compression

- **Color depth**
  Sets the desired color depth. You may select between 8 or 16 bit for Video Optimized/compression level 0, or between 1 and 8 bit for compression level 1 to 9. The higher the color depth, the more video information has to be captured and to be transferred.

5. Usage

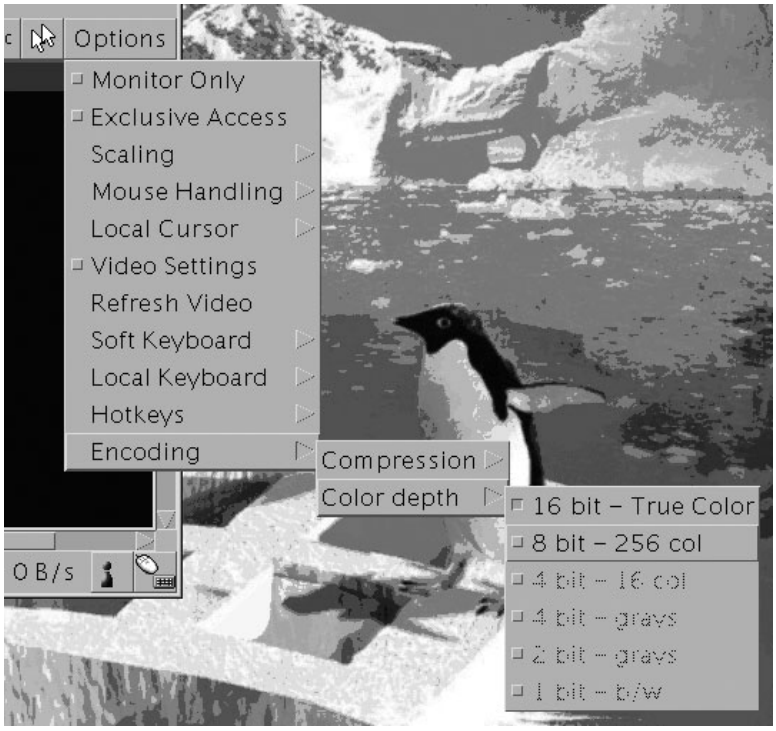


Figure 5-15. Remote Console Options: Color Depth

Note: If displaying motion pictures on a connection with low speed you may achieve an improvement regarding the video transfer rate by lowering the color depth and disabling the option “Video Optimized”. As a general result, the data rate is reduced (less bits per color). Furthermore, the B050-000 will not have to do any video compression. In total, this will lead to less transfer time of the motion picture.

Remote Console Status Line

The status line shows both the console and the connection state. On the left the size of the remote screen is displayed. Figure 5-16 was taken from a Remote Console with a resolution of 800x600 pixels (see Appendix C for a list of screen resolutions that can be displayed using the B050-000). The value in brackets describes the connection to the Remote Console. “Norm” means a standard connection without encryption, “SSL” indicates a secure connection using Secure Socket Layer (SSL).

Figure 5-16. Status Line

5. Usage

The status line displays the number of frame buffer updates (“Fps”) as well as the incoming (“In:”) and the outgoing (“Out:”) network traffic in kilobyte per second. A low value of the network traffic is recommended and can be achieved as described in the Section called Optimizing the Video Picture. If compressed encoding is enabled, a value in brackets displays the compressed transfer rate.

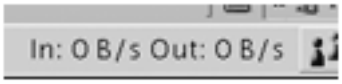


Figure 5-17. Remote Console Options: Color Depth

The next button displays the Remote Console Access settings.

	One single user is connected to the Remote Console of the B050-000.
	One or more users are connected to the Remote Console of the B050-000.
	Exclusive access is set for you. Any other user may not access the remote host via Remote Console unless you disable this option.
	A remote user has exclusive access. You may not access the remote host via Remote Console unless the other user disables this option.

Table 5-3. Buttons displaying the access state

The outer right button displays the state of the Monitor Only settings.

	The option Monitor Only is disabled.
	The option Monitor Only is enabled.

Table 5-4. Buttons displaying the Monitor Only State

For more information about Monitor Only and Exclusive Access settings see the according paragraphs in the Section called “Remote Console Control Bar”.

5. Usage

Optimizing the Video Picture

To achieve an optimal video picture for the Remote Console you may follow the steps as given here:

1. Press the Auto Adjust button once (see the Section called Remote Console Control Bar for details).

2. Choose the option “Video Settings” from the Options Menu of the Remote Console. Press the button “Reset this Mode”.

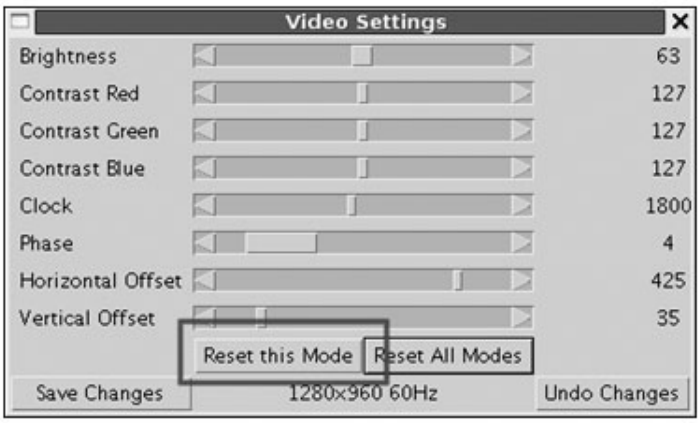


Figure 5-18. Remote Console Video Settings: Reset this Mode

3. Again, press the Auto Adjust button once.

4. The B050-000 detects the video mode with 8 bits (256 colors) automatically. To improve the picture quality you may select 16 bit (True Color) from the Options Menu of the Remote Console, sub menu “Encoding”, entry “Color Depth” (see the Section called “Encoding” for details).

5. Finally, if the Remote Console transfer rate is too high you may do an adjustment using the Noise filter. The higher the filter level the more information is filtered from the transferred video picture (see the Section called “Video” in Chapter 6 for details) and the data rate is reduced.

Currently, the video picture with the best quality can be achieved with the settings “16 bit (High Color)” in the Remote Console or “LAN (High Color)” in the web frontend. This option can also be preset in the Section called “User Console” in Chapter 6.

The sub menu “Compression” from the Options menu has no influence on the picture quality but on the data rate of the picture that is transferred to the Remote Console.

Reducing the Noise of the Video Picture

To reduce the noise from the video picture for the Remote Console you may adjust the Noise filter. Prior to that we recommend you optimize the video picture as described in the Section called Optimizing the Video Picture. In most cases the rate of transferred data indicates the noise level. The higher the transfer rate, the higher the noise of the video picture. You may do an adjustment using the Noise filter. The higher the filter level the more information is filtered from the transferred video picture (see the Section called “Video” in Chapter 6 for details) and the data rate is reduced.

5. Usage

Using the B050-000 with Low Bandwidth

The network connection of the B050-000 has a big influence on the amount of time between two single frames of video. On a connection with low bandwidth it takes longer to transfer the video data from the B050-000 to the Remote Console on the local host. If the remote screen changes, a new picture is sent. In terms of transfer time there is no difference between text screens and screens in graphics mode. The video picture is taken as graphics data no matter what the screen looks like and whichever video mode is chosen. In terms of transferred data there can be an improvement. The compression plays an important role here. You can choose a compression level from the sub menu “Compression” in the Options menu of the Remote Console. Please note that the video will be compressed on the B050-000, transferred to the Remote Console and unpacked in a Java environment. Depending on the remote host and on the local machine this procedure may take some time and may result in a slow updating picture in the Remote Console. To improve the speed you may also set the picture quality in the Remote Console to either “8 bit” or even to grayscale. Because less video data is processed, this is likely to be more effective than the highest compression level.

6. Menu Options

Remote Control

KVM Console

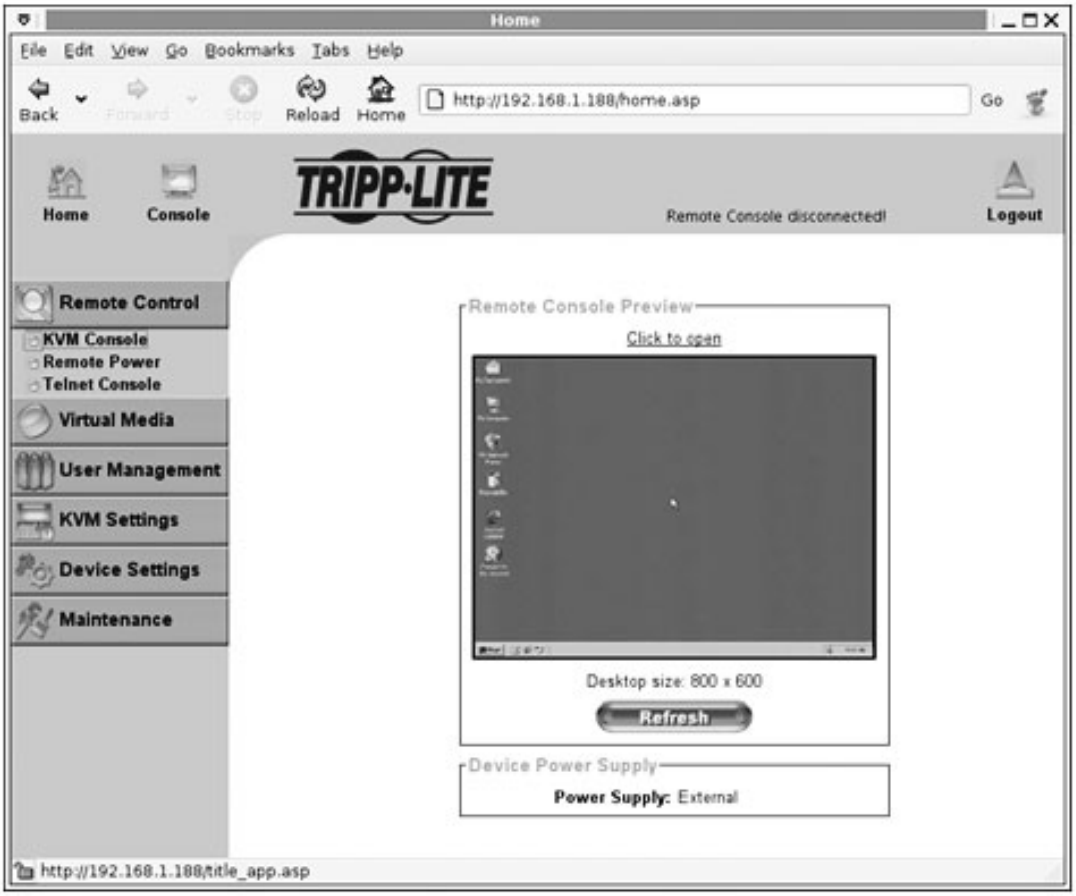


Figure 6-1. KVM Console

Remote Console Preview:

To open the KVM console, either click on the menu entry on the left or on the console picture on the right. To refresh the picture, click on the “Refresh” button.

6. Menu Options

Remote Power

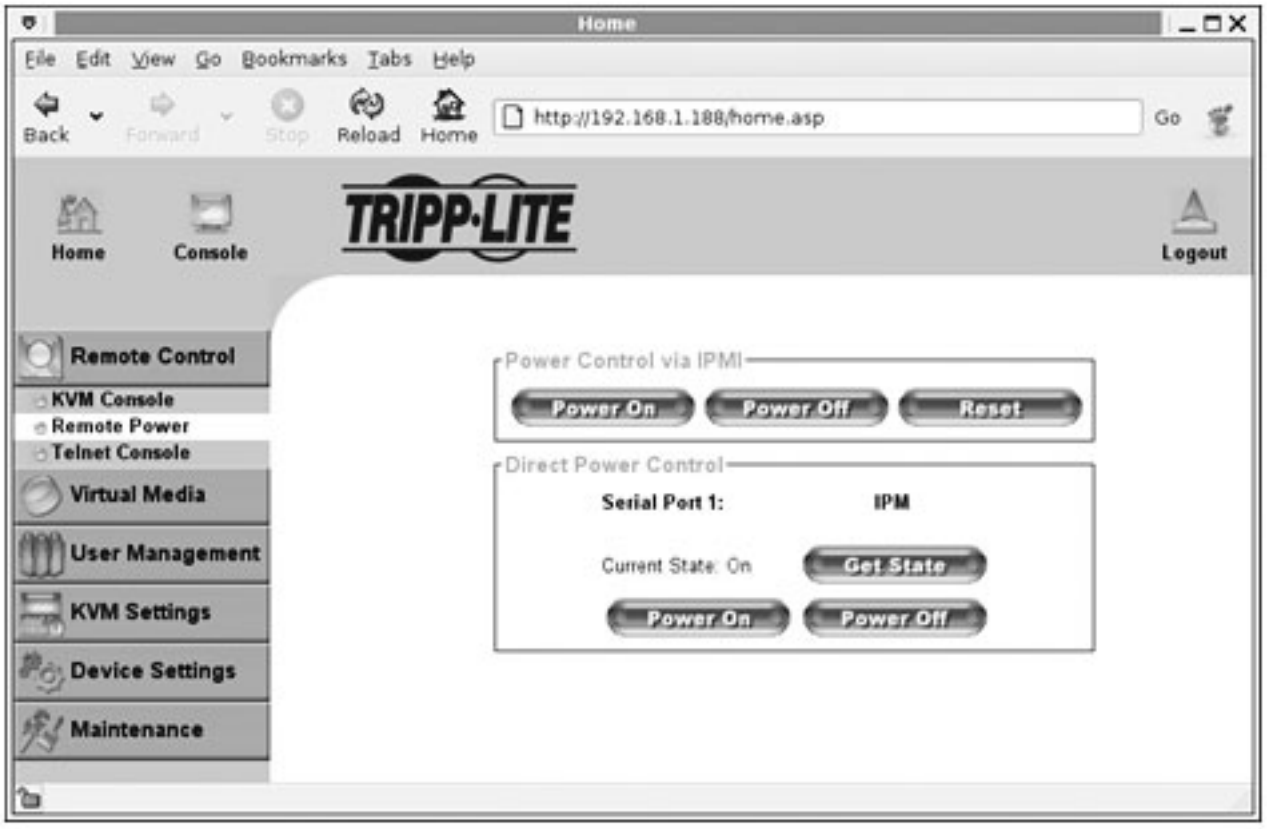


Figure 6-2. B050-000 Power Buttons

Intelligent Platform Management Interface (IPMI)

The B050-000 is capable of controlling the power status of an IPMI-enabled host system. See the Section called "Intelligent Platform Management Interface (IPMI)" for configuration instructions.

If the B050-000 is configured to act as an IPMI client the Remote Power Control page will show three buttons:

Power On:

Sends an IPMI "Power On" command to the Baseboard Management Controller (BMC).

Power Off:

Sends an IPMI "Power Off" command to the BMC.

Reset:

Sends an IPMI "Hard Reset" command to the BMC.

6. Menu Options

Telnet Console

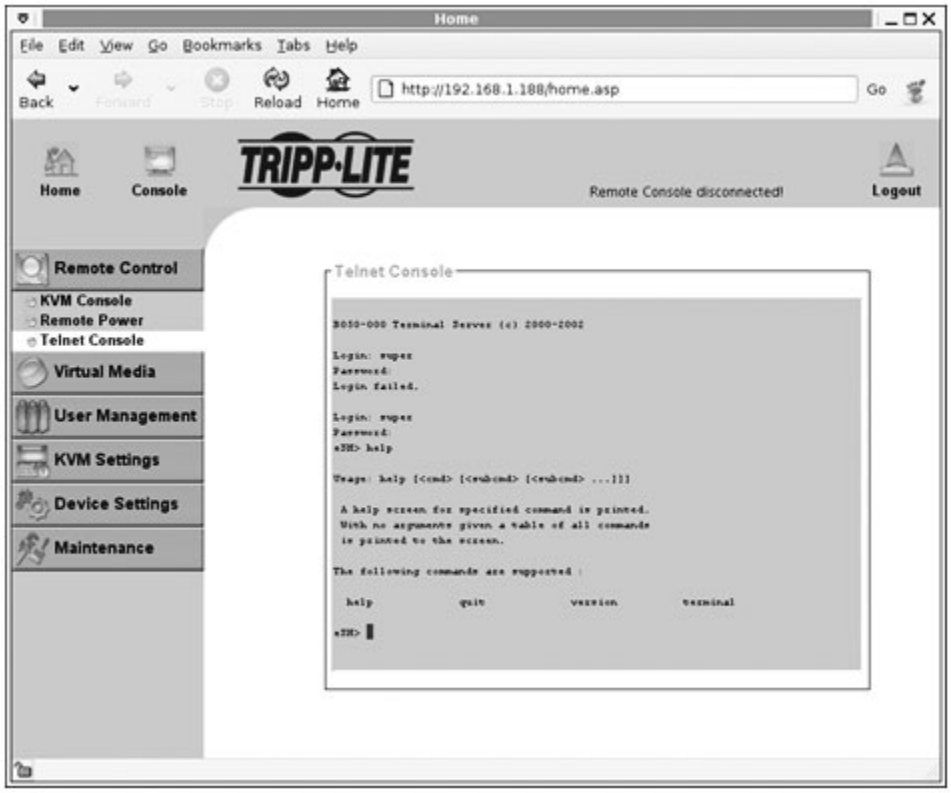


Figure 6-3. Telnet Console

The B050-000 firmware features a Telnet gateway that enables a user to connect to the B050-000 via a standard Telnet client.

For connecting to the B050-000 via Telnet protocol you may use a terminal program such as xterm, TeraTerm or Putty. As an alternative you may also enter the telnet command on the command line or use the “Run” dialog from the Windows Start Menu. As an example you may type the following sequence:

telnet 192.168.1.22

Replace the IP address by the one that is actually assigned to the B050-000. This will prompt for user name and password in order to log into the device. The credentials that need to be entered for authentication are identical to those of the web interface. That means the user management of the Telnet interface is entirely controlled with the functions of the web interface. Once you have successfully logged into the B050-000 a command line will be presented and you can enter the appropriate management commands. In general, the Telnet interface supports two operation modes: the command line mode and the terminal mode. The command line mode is used to control or display some parameters. In terminal mode the pass-through access to serial port 1 is activated (if the serial settings were made accordingly). To access the B050-000 via serial interface both a serial port replicator cable and a null modem cable are required (available separately). All inputs are redirected to the device on serial port #1 and its answers are displayed on the Telnet interface.

6. Menu Options

The following list shows the command syntax and their usage.

Help
Displays the list of possible commands

Quit
Exits the current session and disconnects from the client

Version
Displays the release information

Terminal
Starts the terminal pass-through mode for serial port #1. The key sequence esc exit switches back to the command mode. The command has an optional parameter (1 or 2) to select the desired serial port for pass-through access.

Virtual Media

Floppy Disk

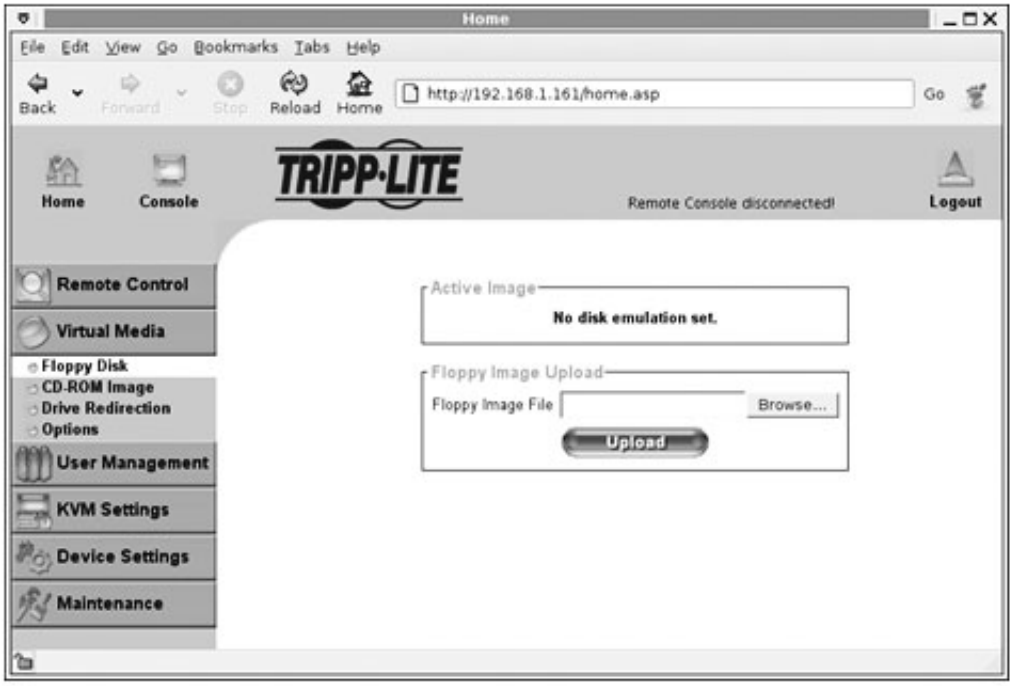


Figure 6-4. Virtual Floppy Area

6. Menu Options

Upload a Floppy Image

Two simple steps enable the user to work on the basis of a certain (floppy) image.

- First the path of the image has to be specified. You can do that either by hand or by using the file selection dialog of your web browser. To open the file selection dialog click on the button “Browse” and select the desired image file.

Figure 6-5. Select Image File

The maximum image size is limited to 1.44MB. To use a larger image, mount this image via Windows Share (or SAMBA) (see the Section called Use Image on Windows Share (SAMBA) for details).

- Then click on the button “Upload” to initiate the transfer of the chosen image file into the B050-000's on-board memory. This image file is kept in the on-board memory of the B050-000 until the end of the current session, until you log out or initiate a reboot of the B050-000.

Download a Floppy Image

A floppy image kept in the B050-000's memory can be both read and written to. To retrieve the changed image contents after writing to it, click the “Download” button and select a folder to store the file in.

Figure 6-6. Active Image File

6. Menu Options

CD-ROM

Use Image on Windows Share (SAMBA)

To include an image from a Windows share select “CD-ROM” from the submenu.

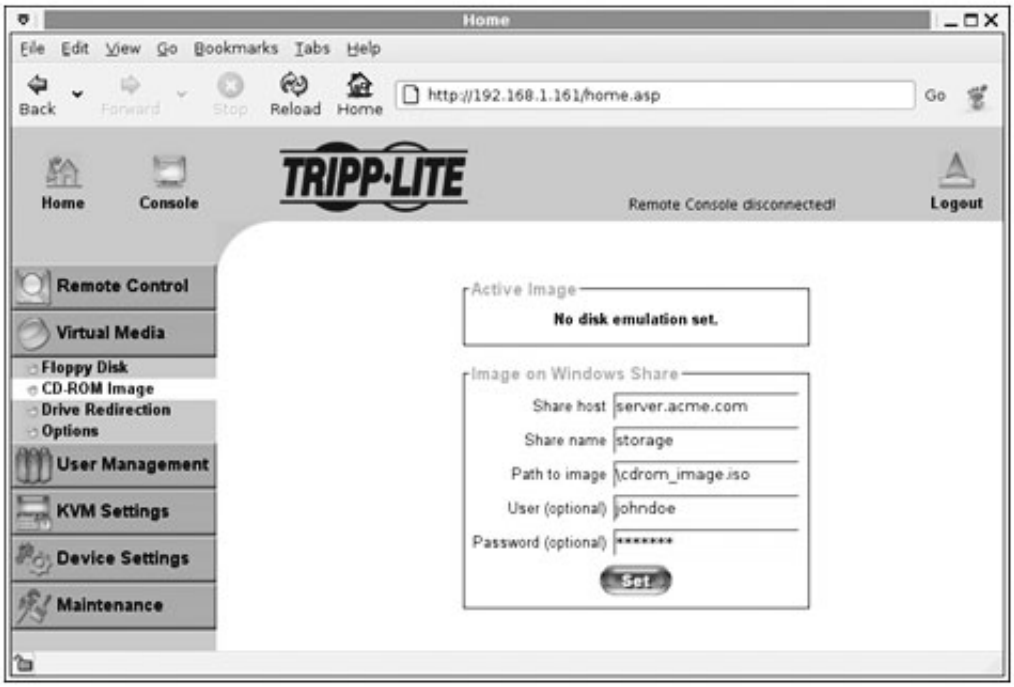


Figure 6-7. Selecting CD-ROM and Windows Share

The following information has to be given to mount the selected image properly:

Share host:

The server name or its IP address. On Windows 95, 98 and Windows ME do not specify the IP address but the server name (“NetBIOS Name”).

Share name:

The name of the share to be used.

Path to image:

The path of the image file on the share.

User (optional):

If necessary, specify the user name for the share named. If unspecified and a guest account is activated, this guest account information will be used as your login.

Password (optional):

If necessary, specify the password for the given user name.

First, the B050-000 will look for a server named mysql.acme.com. Then, the entered share name is selected (in our example we use the share storage) and the image file \cdrom_image.iso is opened. If this file can only be accessed with both a user name and password enter the correct values in the input fields for user name and password. In our case the file is owned by the user "johndoe" and protected by an user-specific pass-phrase (displayed as a number of stars). To register the specified file image and its location click on the button "Set". The specified image file is supposed to be accessible from the B050-000. The information above has to be given from the point of view of the B050-000. It is important to specify correct IP addresses and device names. Otherwise, the B050-000 may not be able to access the referenced the image file properly. Leave the given file unmounted and it will display an appropriate error message instead. So, we recommend that you state the correct values and repeat this step if necessary.

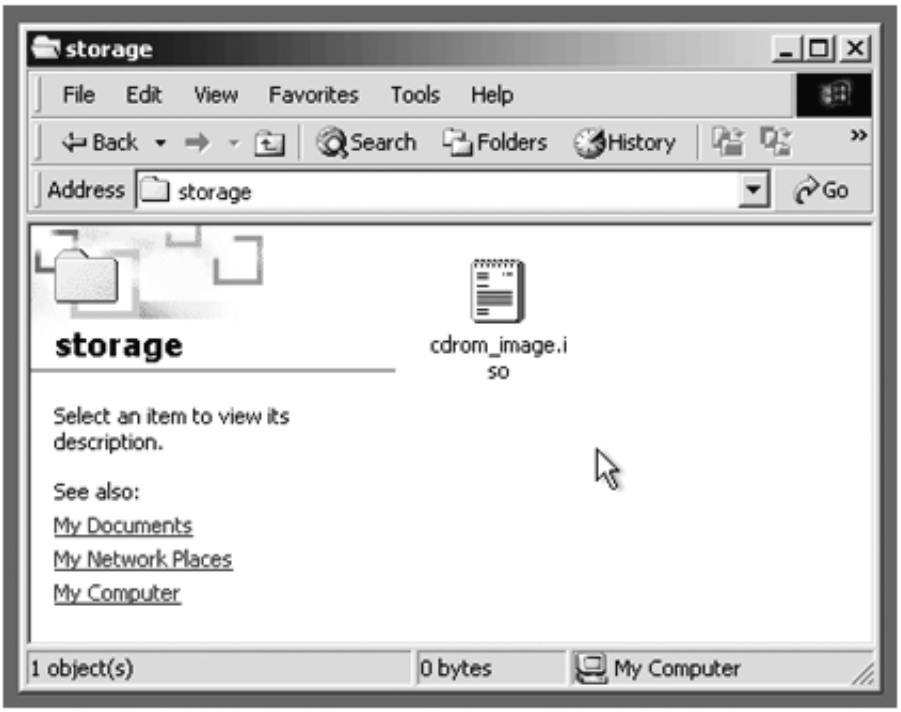


Figure 6-8. The Image File on the Share

Furthermore, the specified share has to be configured correctly. Therefore, administrative permissions are required. As a regular user you may not have these permissions. You should either login as a system administrator (or as "root" on UNIX systems) or ask your system administrator for help to complete this task.

Windows 2000/XP:

Open the Explorer, navigate to the directory (or share) and press the right mouse button to open the context menu. Select "Sharing" to open the configuration dialog (see Figure 6-9).

6. Menu Options

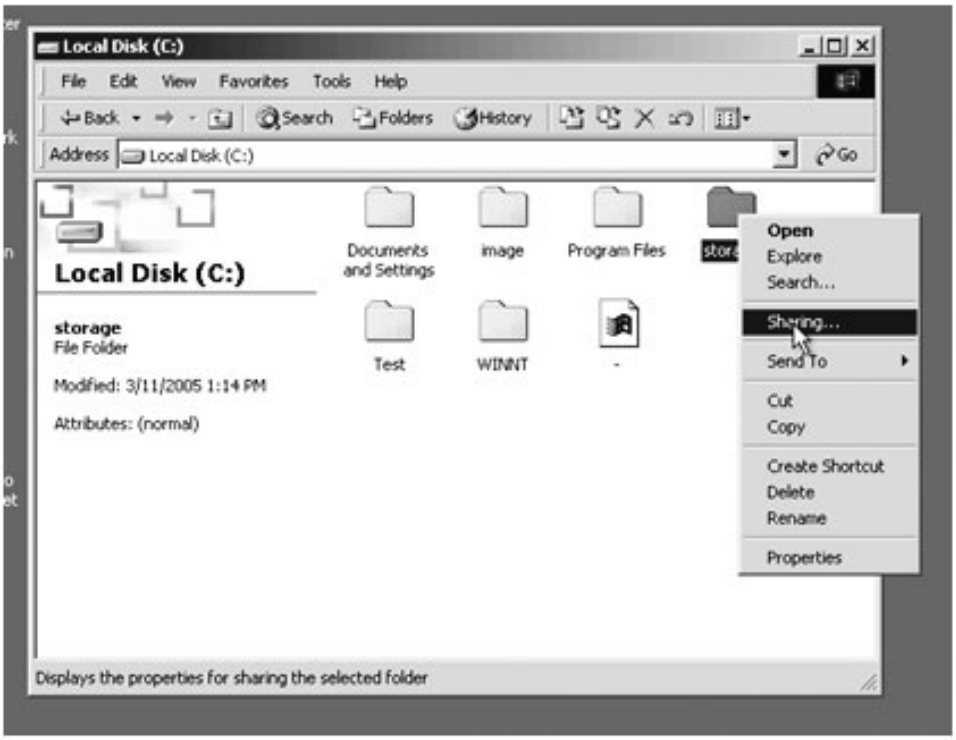


Figure 6-9. Explorer Context Menu

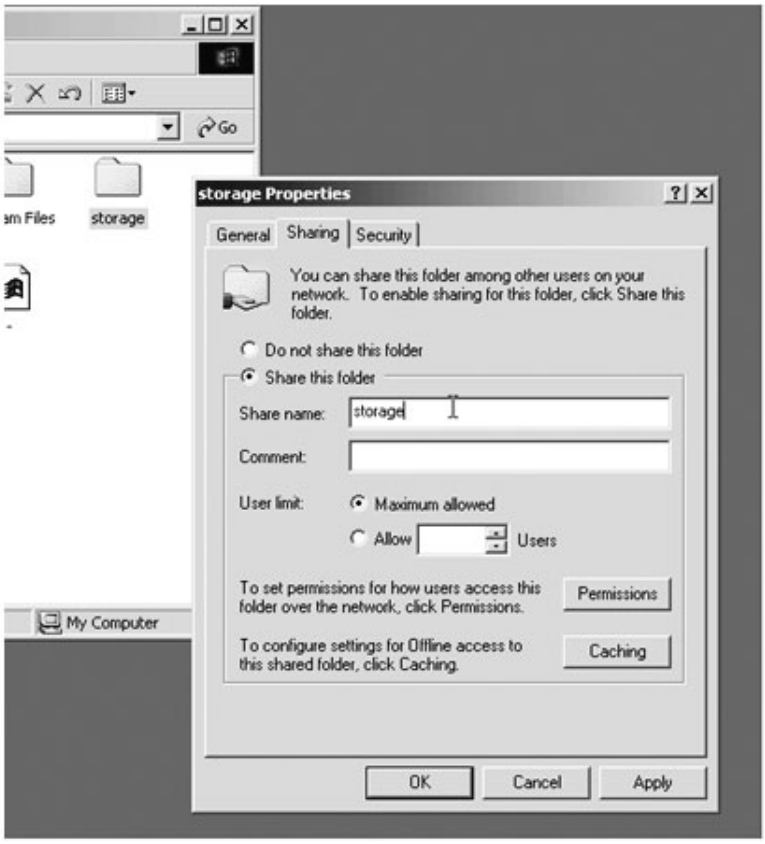


Figure 6-10. Share Configuration Dialog

Adjust the settings for the selected directory.

- Activate the selected directory as a share. Select “Share this folder”.
- Choose an appropriate name for the share. You may also add a short description for this folder (input field “Comment”).
- If necessary, adjust the permissions (button “permissions”).
- Click “OK” to set the options for this share.

UNIX and UNIX-like OS (UNIX, Solaris, Linux):

If you like to access the share via SAMBA, SAMBA has to be set up properly. You may either edit the SAMBA configuration file /etc/samba/smb.conf or use the Samba Web Administration Tool (SWAT) or WebMin to set the correct parameters.

For additional options see the Section called Options for details.

Drive Redirection

Note: Driver redirect requires the B050-000 to be connected via the USB port to the PC or to a USB KVM.

The Drive Redirection is another way to use a virtual disc drive on the remote computer. With Drive Redirection you do not have to use an image file but may work with a drive from your local computer on the remote machine. The drive is hereby shared over a TCP network connection. Devices such as floppy drives, hard discs, CD ROMs and other removable devices like USB sticks can be redirected. It is even possible to enable a write support so that the remote machine can write data to your local disc.

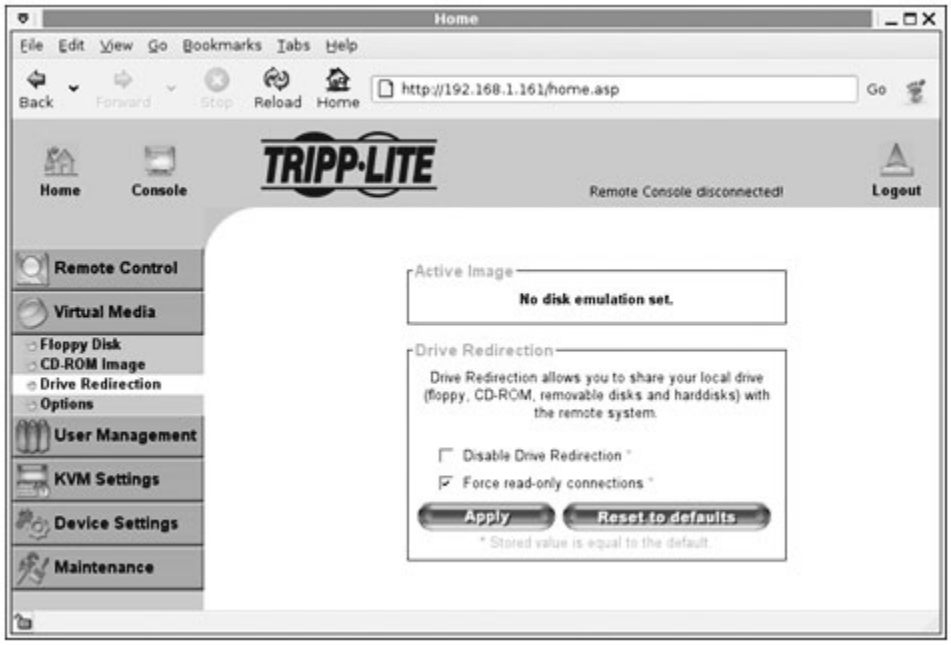


Figure 6-11. Drive Redirection

6. Menu Options

Please note that Drive Redirection works on a level that is far below the operating system. That means that neither the local nor the remote operating system is aware that the drive is currently redirected. This may lead to inconsistent data as soon as one of the operating systems (either from the local machine, or from the remote host) is writing data on the device. If write support is enabled the remote computer might damage the data and the file system on the redirected device. On the other hand, if the local operating system writes data to the redirected device the drive cache of the operating system of the remote host might contain older data. This may confuse the remote host's operating system. We recommend using the Drive Redirection with care, especially the write support.

Drive Redirection Options

As shown in Figure 6-11 the following options may be enabled:

Disable Drive Redirection:
If selected, the Drive Redirection is switched off.

Force Read-Only Connections:
If enabled, the Write Support for the Drive Redirection is switched off. It is not possible to write on a redirected device.

Click "Apply" to submit your changes.

Software Requirements

To use this feature, you have to install the Drive Redirection software that is currently only available for Microsoft Windows. This software can be found on the product CD ROM.

6. Menu Options

Configuration

Figure 6-12. Main View

Specify the parameters of the network connection (see Figure 6-12).

Device:

This is the address (either the DNS name or the IP address) of the B050-000 you would like to connect to.

Port:

This is the network port. By default, B050-000 uses the remote console port (#443) here. You may change this value if you have changed the remote console port in your B050-000's network settings.

Secure Connection:

Enables this box to establish a secure connection via SSL. This will maximize the security but may reduce the connection speed.

6. Menu Options

Drive Selection

Figure 6-13. Selecting the Desired Drive

Select the drive you would like to redirect. All available devices (drive letters) are shown here. Please note that the whole drive is shared with the remote computer, not only one partition. If you have a hard disk with more than one partition all drive letters that belong to this disk will be redirected. The Refresh button may be used to regenerate the list of drive letters, especially for a USB stick.

6. Menu Options

Write Support

Figure 6-14. Selecting Write Support

This feature may be enabled here. Write support means that the remote computer is allowed to write on your local drive. As you can imagine, this is very dangerous. If both the remote and the local system try to write data on the same device, it will certainly destroy the file system on the drive. Please use this only when you're sure what you are doing.

Warning: Using drive redirection with the write support option enabled is an experimental feature and poses great danger to the data contianed on the shared drive. Use this feature at your own risk.

6. Menu Options

Device Authentication

Figure 6-15. Device Authentication

To use the Drive Redirection, you have to authenticate on the B050-000 using a valid username and password. Permission to change the virtual disc configuration is necessary.

Navigation Buttons

Connect/Disconnect:

To establish the drive redirection, press the Connect button once. If all the settings are correct, the status bar displays that the connection has been established, the Connect button is disabled and the Disconnect button is enabled. On an error, the status line shows the error message. The drive redirection software tries to lock the local drive before it is redirected. That means that it tries to prevent the local operating system from accessing the drive as long as it is redirected. This may also fail, especially if a file on the drive is currently open. In the case of a locking failure, you will be prompted if you want to establish the connection anyhow. This should not be a serious problem when the note above is respected. If the write support is enabled, a drive which is not locked might be damaged by the Drive Redirection.

With the Disconnect button, a connection via Drive Redirection connection is stopped.

Exit/Hide:

If the Exit button is pressed, the Drive Redirection software is closed. If a Drive Redirection connection is active, the connection will be closed before the application terminates.

Using the Hide to Tray button the application is hidden, but not terminated completely. That means that an active connection will be kept active until it is closed explicitly. You can access the software by its tray icon. The tray icon also shows whether a connection is established or not. A double click on the icon shows the application window, or with a right click you may access a small menu (see Figure 6-16).

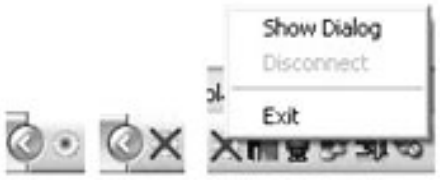


Figure 6-16. Tray Info

Options

Figure 6-17. USB Mass Storage Option

Set this option to disable the mass storage emulation (and hide the virtual drive) as long as no image file is currently loaded. If unset and no file image is found, it may happen that the host system will hang on boot because of changes in the boot order or the boot manager (LILO, GRUB). This case has been seen for some Windows versions (2000, XP). Other OS may not be fully excluded. This behavior depends on the BIOS version used in that machine.

To set this option, press the button “Apply”.

Creating an Image

Floppy Images

UNIX and UNIX-like OS:

To create an image file make use of “dd”. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, Linux). To create a floppy image file, copy the contents of a floppy to a file. You can use the following command:

dd [if=/dev/fd0] [of=/tmp/floppy.image]
dd reads the entire disc from the device /dev/fd0 and saves the output in the specified output file /tmp/floppy.image. Adjust both parameters exactly to your needs (input device etc.)

MS Windows:

You can use the tool “Raw Write for Windows”.

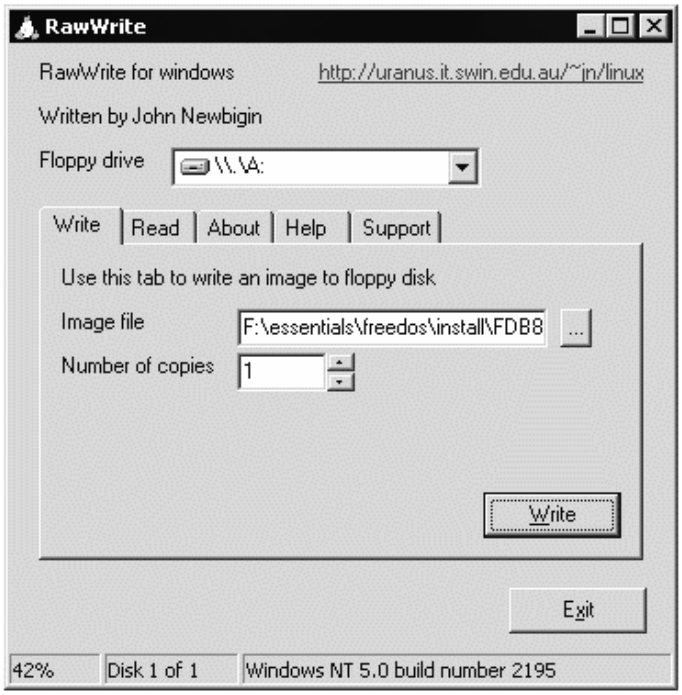


Figure 6-18. RawWrite for Windows Selection Dialog

Select the tab “Read” from the menu. Enter (or choose) the name of the file in which you would like to save the floppy content. Click on the button “Copy” to initiate the image creation process.

For related tools, look at the homepage of the fdos project (http://www.fdos.org/ripcord/rawrite/).

CD-ROM/ISO 9660 Images

UNIX and UNIX-like OS:

Make use of “dd” to create an image file. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, Linux).

To create a CDROM image file, copy the contents of the CDROM to a file. You can use the following command:

dd [if=/dev/cdrom] [of=/tmp/cdrom.image]

dd reads the entire disc from the device /dev/cdrom and saves the output in the specified output file /tmp/cdrom.image. Adjust both parameters exactly to your needs (input device etc.).

MS Windows:

To create the image file, use your preferred CD imaging tool. Copy the whole contents of the disc into one single ISO image file on your hard-disk. For example, with “Nero” you choose “Copy and Backup”. Then, navigate to the “Copy Disc” section. Select the CD ROM or DVD drive from which you would like to create an ISO image. Specify the filename of the ISO image and save the CD ROM content in that file.

Figure 6-19. Nero Selection Dialog

6. Menu Options

User Management

Change Password

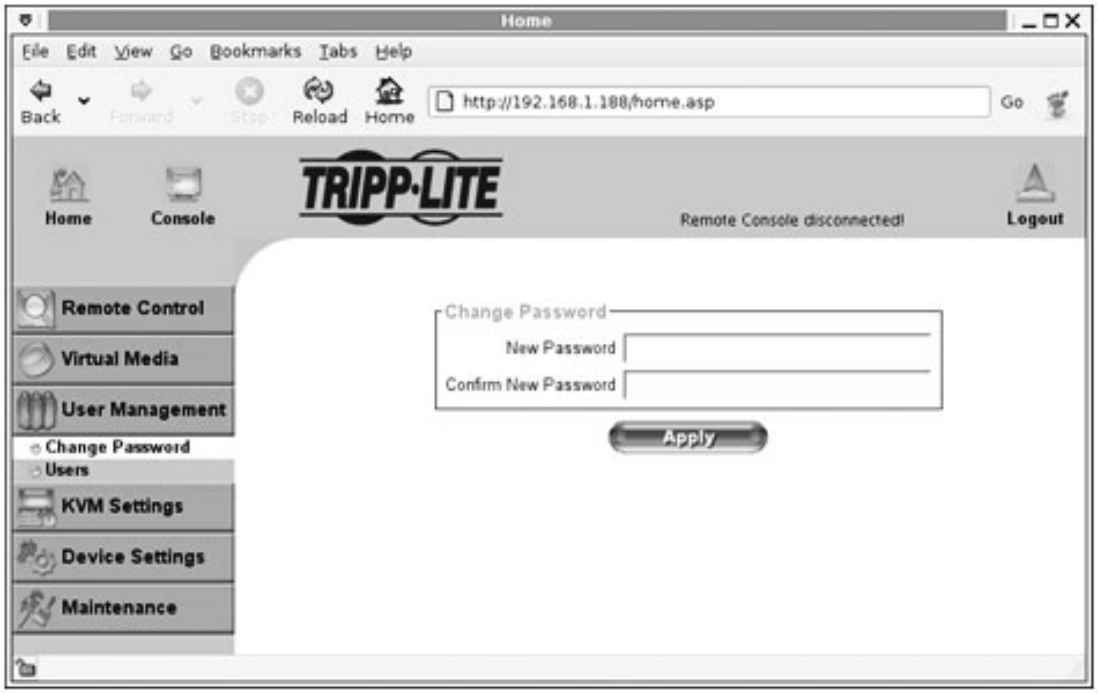


Figure 6-20. Set Password

To change your password, enter the new password in the upper entry field. Retype the password in the field below.

Click “Apply” to submit your changes.

6. Menu Options

Users And Groups

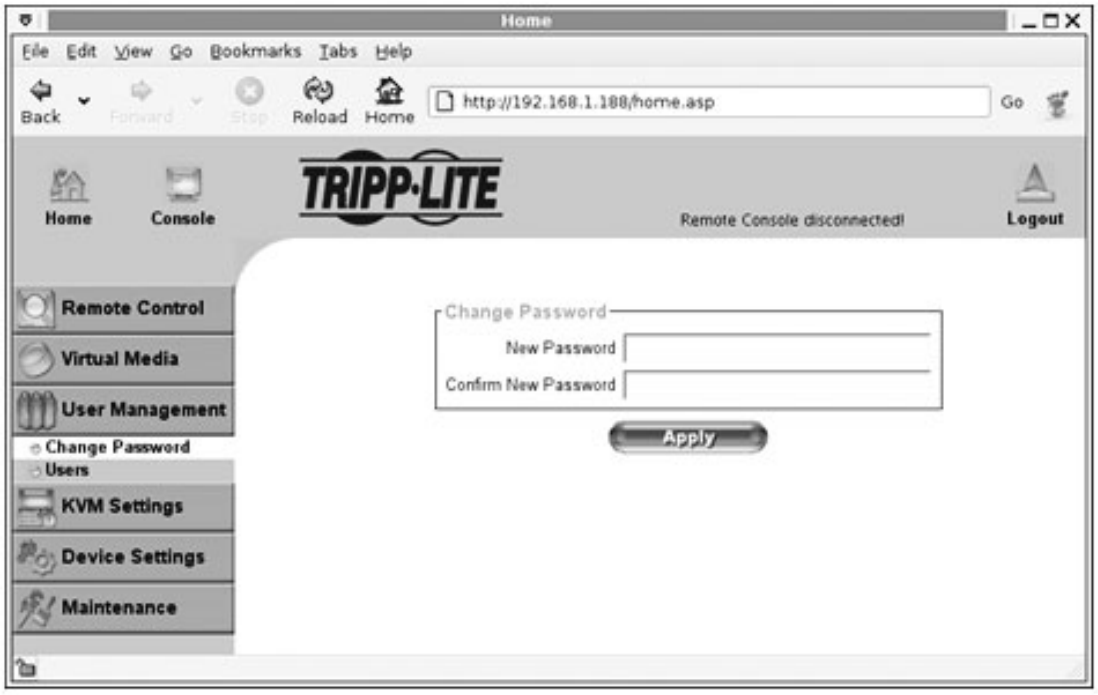


Figure 6-21. Set Use

User Management

The B050-000 comes with a pre-configured user account for the user “super” that has fixed permissions. This user has all possible rights to configure the device and to use all functions the B050-000 offers.

Upon delivery, the account for the user “super” has the password “pass”. Make sure to change the password immediately after you have installed and accessed your B050-000 for the first time. A full list of available options follows. This list can only be seen by the Superuser.

Existing users:
Select an existing user for modification. Once a user has been selected, click the lookup button to see the user information.

New User name:
The new user name for the selected account.

Password:
The password for the login name. It must be at least four characters long.

Confirm password:
Confirmation of the password above.

Email address:
This is optional.

Mobile number:

This is also optional.

Role:

Each user can be a member of a group (named a “role”) - either an administrator, or a regular user. Choose the desired role from the selection box.

To create a user, press the button “Create”. The button “Modify” changes the displayed user settings. To delete a user press the button “Delete”.

Note: The B050-000 is equipped with a host-independent processor and memory unit both of which have a limitation in terms of the processing instructions and memory space. To guarantee an acceptable response time, we recommend not to exceed 25 users connected to the B050-000 at the same time. The memory space that is available on the B050-000 depends primarily on the configuration and the usage of the B050-000 (log file entries etc.). That's why we recommend not to store more than 150 user profiles.

KVM Settings

User Console

The following settings are user specific. That means the Super User can customize these settings for every users separately. Changing the settings for one user does not affect the settings for the other users.

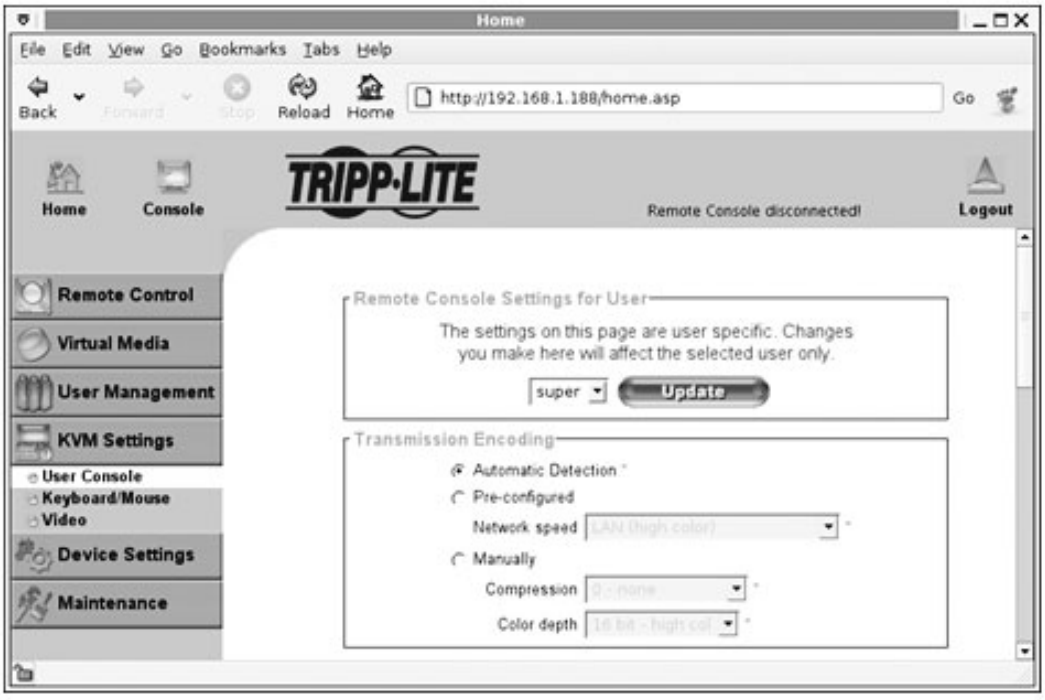


Figure 6-22. User Console Settings (Part 1)

6. Menu Options

Remote Console Settings for User

This selection box displays the user ID for the values shown and for the changes that will take effect. Select the desired user from the selection box and press the button “Update”. The user settings will be displayed below.

Note: You are allowed to change the settings of other users only if you have the necessary access rights for this task. For a regular user without the correct permissions it is not possible to change the settings for any other users.

Transmission Encoding

The Transmission Encoding setting allows you to change the image-encoding algorithm that is used to transmit the video data to the Remote Console window. It is possible to optimize the speed of the remote screen depending on the number of users working at the same time and the bandwidth of the connection line (Modem, ISDN, DSL, LAN, etc.).

Automatic detection:

The encoding and the compression level is determined automatically from the available bandwidth and the current content of the video image.

Pre-configured:

The pre-configured settings deliver the best result because of optimized adjustment of compression and color depth for the indicated network speed.

Manually:

Allows you to adjust both compression rate and the color depth individually. Depending on the selected compression rate, the data stream between the B050-000 and the Remote Console will be compressed in order to save bandwidth. Since high compression rates are very time consuming, they should not be used while several users are accessing the B050-000 simultaneously.

The standard color depth is 16 Bit (65536 colors). The other color depths are intended for slower network connections in order to allow a faster transmission of data. Therefore compression level 0 (no compression) uses only 16 Bit color depth. At lower bandwidths, only 4 Bit (16 colors) and 2 Bit (4 gray scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4 Bit (16 gray scales). 1 Bit color depth (black/white) should only be used for extremely slow network connections.

6. Menu Options

Remote Console Type

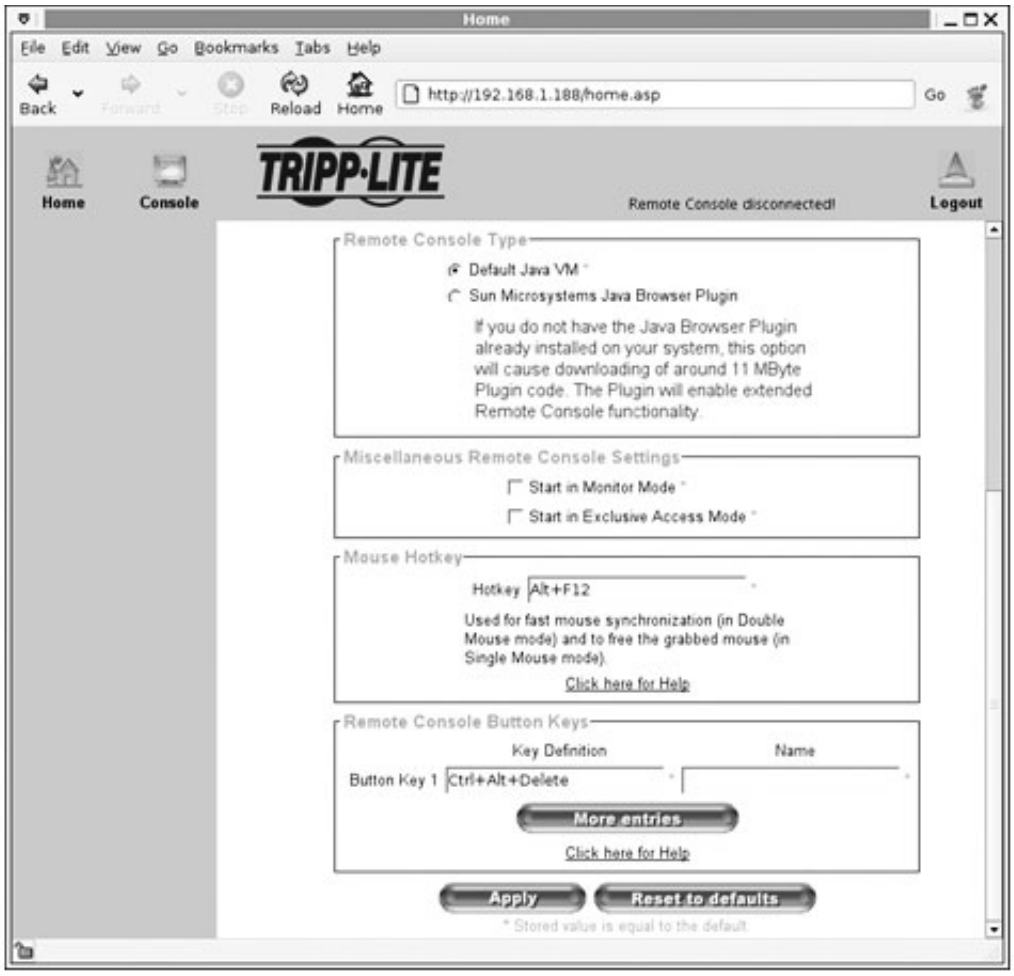

Home
File Edit View Go Bookmarks Tabs Help
Back Forward Stop Reload Home
http://192.168.1.188/home.asp
Go
Home
Console
TRIPP·LITE
Remote Console disconnected!
Logout
Remote Console Type
Default Java VM *
Sun Microsystems Java Browser Plugin
If you do not have the Java Browser Plugin already installed on your system, this option will cause downloading of around 11 MByte Plugin code. The Plugin will enable extended Remote Console functionality.
Miscellaneous Remote Console Settings
Start in Monitor Mode *
Start in Exclusive Access Mode *
Mouse Hotkey
Hotkey Alt+F12 *
Used for fast mouse synchronization (in Double Mouse mode) and to free the grabbed mouse (in Single Mouse mode).
Click here for Help
Remote Console Button Keys
Key Definition
Name
Button Key 1 Ctrl+Alt+Delete
More entries
Click here for Help
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 6-23. User Console Settings (Part 2)

Specifies which Remote Console Viewer is to be used.

Default Java Virtual Machine (JVM):

Uses the default JVM of your web browser. This may be the Microsoft JVM for the Internet Explorer or the Sun JVM if it is configured this way. Use of the Sun JVM may also be forced (see below).

Sun Microsystems Java Browser Plugin:

Instructs the web browser of your administration system to use the JVM of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console window, which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not yet installed on your system, it may be downloaded and installed automatically. However, in order to make the installation possible, you still have to answer the appropriate dialogs with “yes”. The download volume is around 11 Mbytes. The advantage of downloading Sun's JVM is the usage of a stable and identical JVM across different platforms. The Remote Console software is optimized for this JVM version and offers a wider range of functionality when run in SUN's JVM.

(Hint: If you are connected over a slow connection to the Internet you can also pre-install the JVM on your administration machine)

Miscellaneous Remote Console Settings

Start in Monitor Mode:

Sets the initial value for the monitor mode. By default the monitor mode is disabled. If you switch it on, the Remote Console window will be started in a read only mode.

Start in Exclusive Access Mode:

Enables the exclusive access mode immediately at Remote Console startup. This forces the Remote Consoles of all other users to close. Nobody else can open the Remote Console at the same time again until you disable this feature or log off.

Mouse Hotkey

Allows you to specify a hotkey combination which starts either the mouse synchronization process if pressed in the Remote Console or is used to leave the single mouse mode.

Remote Console Button Keys

Button Keys allow simulating keystrokes on the remote system that cannot be generated locally. The reason for this might be a missing key or in the event that the local operating system of the Remote Console is unconditionally catching this keystroke already. Typical examples are “Control+Alt+Delete” on Windows and DOS, that is always caught, or the key sequence “Control+Backspace” on Linux that can be used for terminating the X-Server.
In order to define a new Button Key or to adjust an existing one, have a look at the rules that describe the setting for a key. In general, the syntax for a key is as follows:

[confirm] <keycode>[+|-|>[*]<keycode>]*

A term in brackets is optional. The star at the end means that you add further keys as often as required for your case. The term “confirm” adds a confirmation dialogue that is displayed before the key strokes will be sent to the remote host.

The “keycode” is the key to be sent. Multiple key codes can be concatenated with either a plus, a minus, or an “>” sign. The plus sign builds key combinations - all the keys will be pressed until a minus sign or the end of the combination is encountered. In this case all pressed keys will be released in reversed sequence. So, the minus sign builds single, separate keypresses and keyreleases. The “>” sign releases the last key, only. The star inserts a pause with a duration of 100 milliseconds.

As an example, the key combination of Ctrl, Alt and F2 is represented by the sequence Ctrl+Alt+F2

For a full list of key codes and aliases please refer to the Appendix E.

Note: If you need more button keys than shown use the button “More entries”. This will open a list of additional entry fields.

6. Menu Options

Keyboard/Mouse

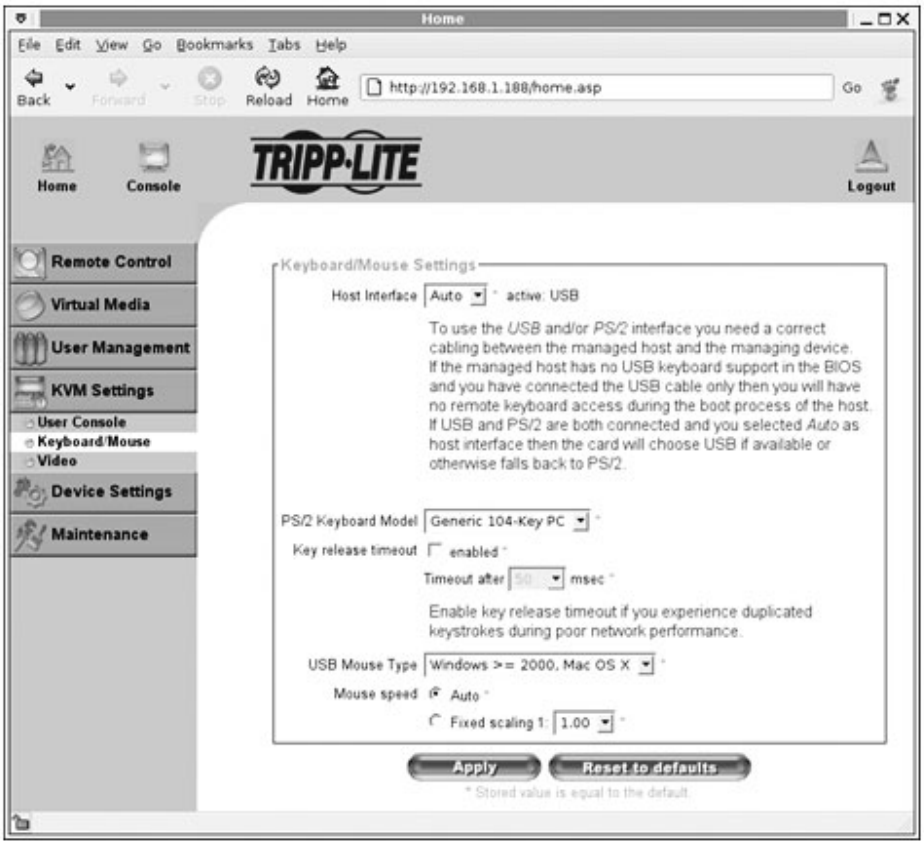

Home
File Edit View Go Bookmarks Tabs Help
Back Forward Stop Reload Home
http://192.168.1.188/home.asp
Go
Home
Console
TRIPP·LITE
Logout
Remote Control
Virtual Media
User Management
KVM Settings
User Console
Keyboard/Mouse
Video
Device Settings
Maintenance
Keyboard/Mouse Settings
Host Interface Auto * active: USB
To use the USB and/or PS/2 interface you need a correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only then you will have no remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you selected Auto as host interface then the card will choose USB if available or otherwise falls back to PS/2.
PS/2 Keyboard Model Generic 104-Key PC *
Key release timeout enabled *
Timeout after msec *
Enable key release timeout if you experience duplicated keystrokes during poor network performance.
USB Mouse Type Windows >= 2000, Mac OS X *
Mouse speed Auto *
Fixed scaling 1: 1.00 *
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 6-24. Keyboard and Mouse Settings

Host Interface

Enables the desired mouse interface. You can choose between "Auto" for automatic detection, "USB" for a USB mouse and "PS/2" for a PS/2 mouse.

Warning: To use the USB and/or PS/2 interface, you need the correct cabling between the managed host and the managing device. If the managed host does not have USB keyboard support in the BIOS and you have connected the USB cable only, then you will not have any remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you selected "Auto" as host interface, then the card will select "USB" if available, otherwise it falls back to "PS/2".

To get USB remote keyboard access during the boot process of the host, the following conditions must be fulfilled:

- The host BIOS must have USB keyboard support
- The USB cable must be connected or must be selected in the Host interface option

PS/2 Keyboard Model

Enables a certain keyboard layout. You can choose between “Generic 101-Key PC” for a standard keyboard layout, “Generic 104-Key PC” for a standard keyboard layout extended by three additional Windows keys, “Generic 106-Key PC” for a Japanese keyboard, and “Apple Macintosh” for the Apple Macintosh. If a keyboard timeout is required, the appropriate option can be enabled. In addition, set the desired time value in the input field below.

USB Mouse Type

Enables the USB mouse type. Choose an appropriate option from the selection box. For a detailed description about the mouse type and recommended options for the different operating systems see the Section called Recommended Mouse Settings in Chapter 4.

Mouse Speed

- **Auto mouse speed**
  Use this option if the mouse settings on the host use an additional acceleration setting. The B050-000 tries to detect the acceleration and speed of the mouse during the mouse sync process.

- **Fixed mouse speed**
  Use a direct translation of mouse movements between the local and the remote pointer. You may also set a fixed scaling which determines the amount the remote mouse pointer is moved when the local mouse pointer is moved by one pixel. This option only works when the mouse settings on the host are linear. This means that there is no mouse acceleration involved.

  To set the options click on the button “Apply”.

6. Menu Options

Video

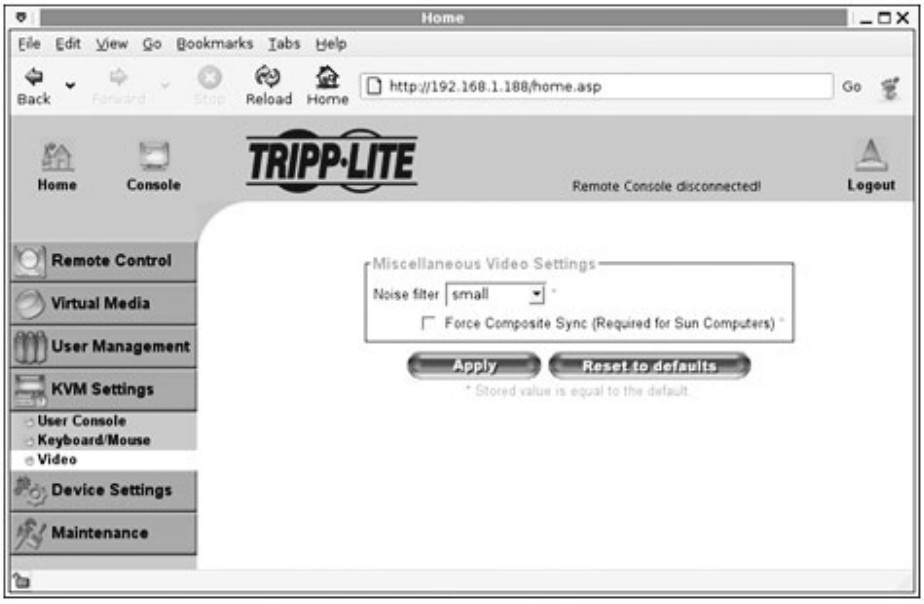


Figure 6-25. Video Settings

To set the options (see below) click on the button "Apply".

Miscellaneous Video Settings

Noise filter:

This option defines how the B050-000 reacts to small changes in the video input signal. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if the display content is not really changing (depending on the quality of the video input signal). All in all, the default setting should be suitable for most situations.

Force Composite Sync (Required for Sun Computers):

Enable this option to support signal transmission from a Sun machine. If not enabled, the picture of the remote console will not be visible.

Device Settings

Network

The Network Settings panel as shown in Figure 6-26 allows changing network related parameters. Each parameter will be explained below. Once applied the new network settings will immediately come into effect.

6. Menu Options

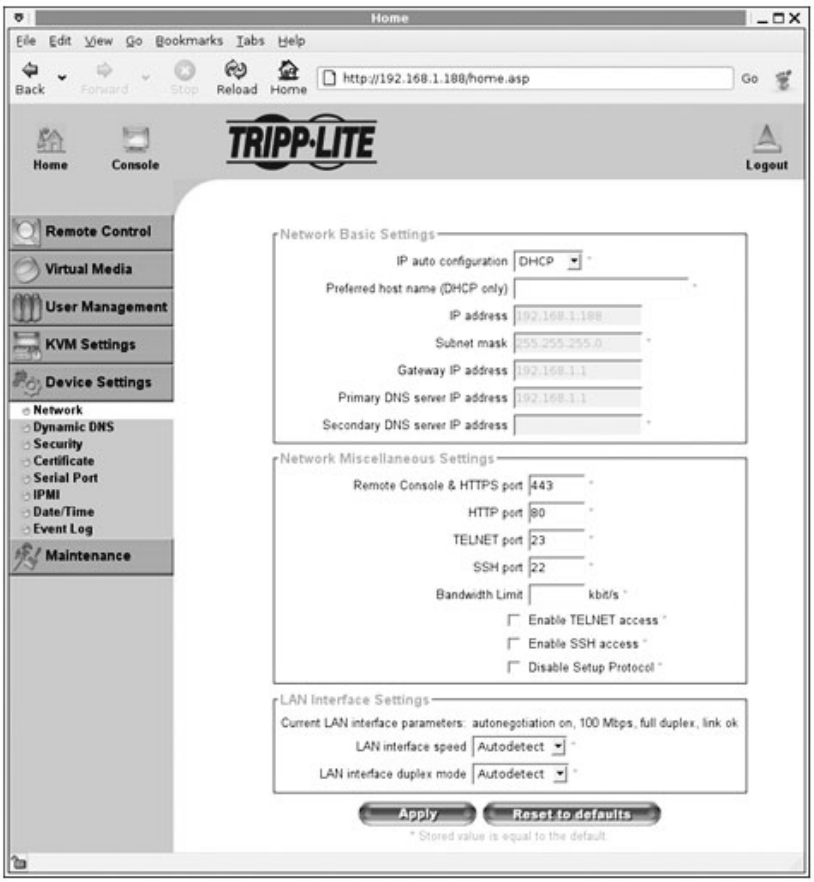


Figure 6-25. Video Settings

Warning: The initial IP configuration is usually done directly at the host system using the special procedure described in Table 4-1.

Warning: Changing the network settings of the B050-000 might result in losing connection to it. If you change the settings remotely, make sure that all the values are correct and you still have an option to access the B050-000.

Basic Network Settings

IP auto configuration

With this option you can define if the B050-000 should fetch its network settings from a DHCP or BOOTP server. For DHCP select “dhcp” and for BOOTP select “bootp”. If you choose “none” then IP auto configuration is disabled.

Preferred host name:
Preferred host name to request from DHCP server. Whether the DHCP server takes the B050-000's suggestion into account or not depends on the server configuration.

IP address:
IP address in the usual dot notation.

Subnet Mask:
The net mask of the local network.

Gateway IP address:
In case the B050-000 should be accessible from networks other than the local one, this IP address must be set to the local network router 's IP address.

Primary DNS Server IP Address:
IP address of the primary Domain Name Server in dot notation. This option may be left empty, however the B050-000 will not be able to perform name resolution.

Secondary DNS Server IP Address:
IP address of the secondary Domain Name Server in dot notation. It will be used in case the Primary DNS Server cannot be contacted.

Miscellaneous Network Settings

Remote Console And HTTPS port:
Port number at which the B050-000's Remote Console server and HTTPS server are listening. If left empty the default value will be used.

HTTP port:
Port number at which the B050-000's HTTP server is listening. If left empty the default value will be used.

Telnet port:
Port number at which the B050-000's Telnet server is listening. If left empty the default value will be used.

SSH port:
Port number at which the B050-000's Secure Shell (SSH) server is listening. If left empty the default value will be used.

Bandwidth Limit:
The maximum network traffic generated through the B050-000 Ethernet device. Value in Kbit/s.

Enable Telnet access:
Set this option to allow accessing the B050-000 using the Telnet gateway (see the Section called Telnet Console).

Enable SSH access:

Set this option to allow accessing the B050-000 using the Secure Shell (SSH) protocol. The SSH console offers the same features as Telnet (see the Section called Telnet Console), but uses a secure, encrypted connection instead.

Disable Setup Protocol:

Enable this option to exclude the B050-000 from the setup protocol.

LAN Interface Settings

This entry field displays the current settings for the Ethernet/LAN interface of the B050-000. You may choose between auto negotiation and a fixed setting for the Ethernet transceiver settings “interface speed” and “duplex mode” in case auto negotiation does not work correctly.

LAN interface speed:

Depending on your network connection you may select a speed value for this interface. To adjust the interface automatically, choose “autodetect” (default value). If this selection results in misbehavior of the interface, choose one of other speed options to be used. The interface will transmit and receive data with that fixed speed.

LAN interface duplex mode:

If necessary, you may also select a specific duplex mode. The default value is set to “autodetect” which leads to an automatic setting of the duplex mode depending on your network (recommended). As an alternative you may explicitly set the interface to either “half duplex” or “full duplex” mode.

These settings may also be configured via a serial console. See the Section called Initial Configuration via Serial Console in Chapter 4 for details.

Dynamic DNS

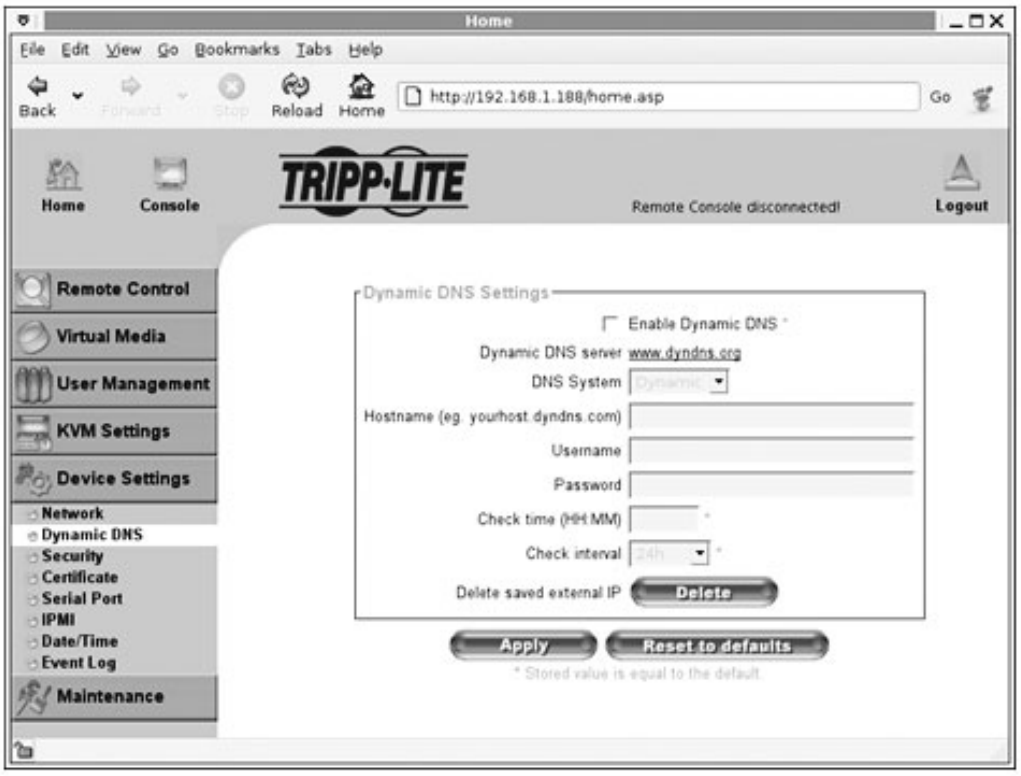


Figure 6-27. Dynamic DNS

A freely available Dynamic DNS service (dyndns.org) can be used in the following scenario (see Figure 6-28):

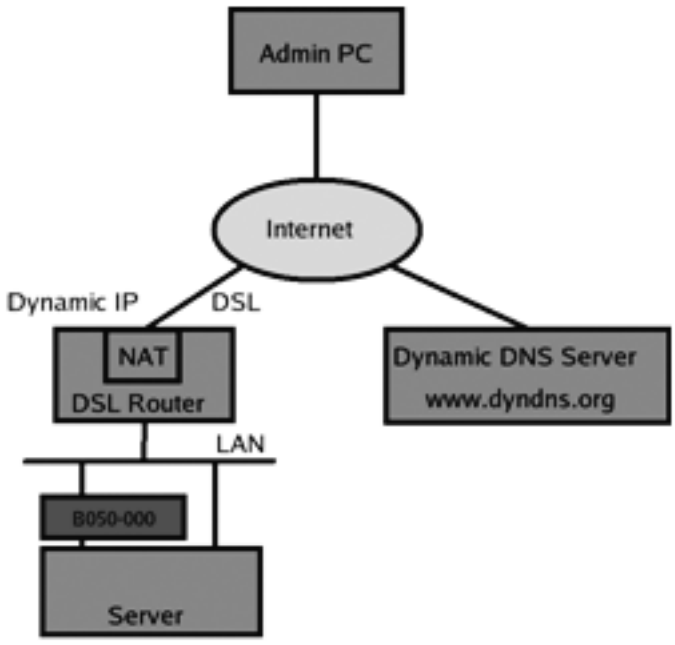


Figure 6-28. Dynamic DNS Scenario

6. Menu Options

The B050-000 is reachable via the IP address of the DSL router, which is dynamically assigned by the provider. Since the administrator does not know the IP address assigned by the provider, the B050-000 connects to a special dynamic DNS server in regular intervals and registers its IP address there. The administrator may contact this server as well and pick up the same IP address belonging to his card. The administrator has to register a B050-000 that is supposed to take part in the service with the Dynamic DNS Server and assign a certain hostname to it. He will get a nickname and a password in return to the registration process. This account information together with the hostname is needed in order to determine the IP address of the registered B050-000. You have to perform the following steps in order to enable Dynamic DNS:

- Make sure that the LAN interface of the B050-000 is properly configured.
- Enter the Dynamic DNS Settings configuration dialog as shown in Figure 6-27.
- Enable Dynamic DNS and change the settings according to your needs (see below).

Enable Dynamic DNS:
This enables the Dynamic DNS service. This requires a configured DNS server IP address.

Dynamic DNS server:
This is the server name where B050-000 registers itself in regular intervals. Currently this is a fixed setting since only dyndns.org is supported for now.

Hostname:
This is the hostname of the B050-000 that is provided by the Dynamic DNS Server. (use the whole name including the domain, e.g. testserver.dyndns.org, not just the actual hostname).

Username:
You have registered this username during your manual registration with the Dynamic DNS Server. Spaces are not allowed in the Nickname.

Password:
You have used this password during your manual registration with the Dynamic DNS Server.

Check time:
The B050-000 card registers itself in the Dynamic DNS server at this time.

Check interval:
This is the interval for reporting again to the Dynamic DNS server by the B050-000.

Warning: The B050-000 has its own independent real time clock. Make sure the time setting of the B050-000 is correct (see the Section called Date And Time).

The option “Delete saved external IP” is useful if you would like to update your IP address saved externally. To delete the saved address, press the button “Delete”.

6. Menu Options

Security

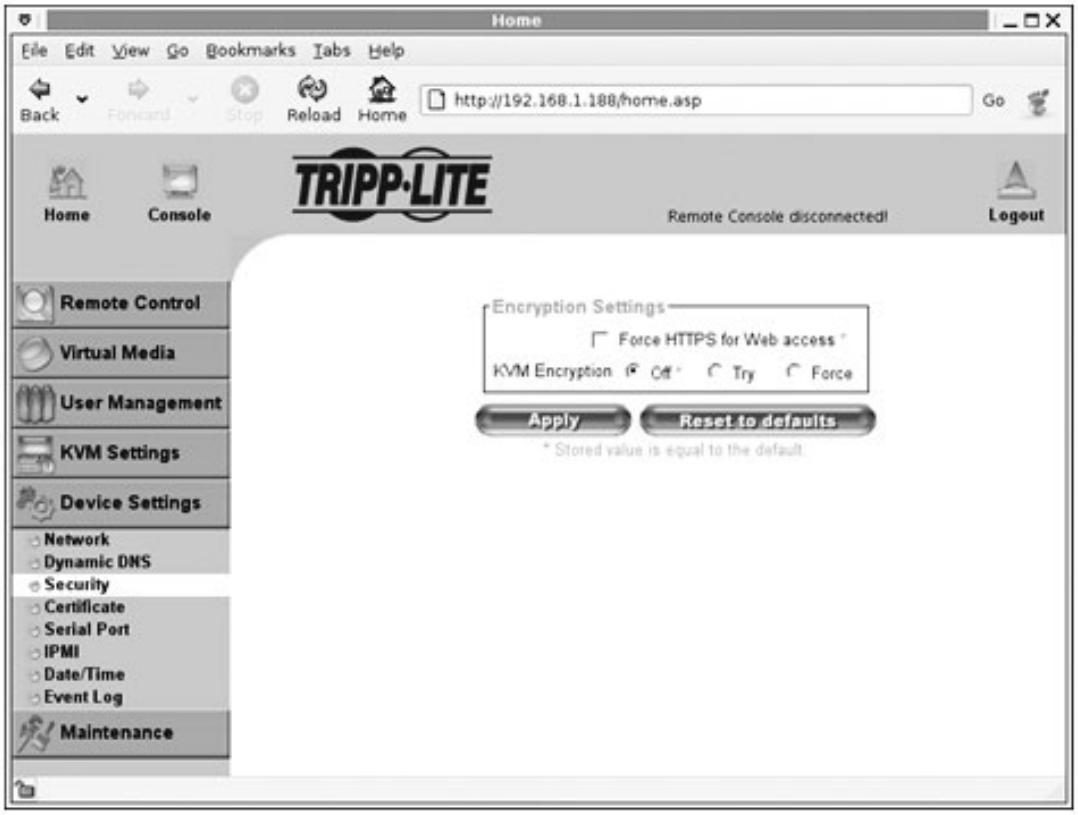


Figure 6-29. Device Security

Encryption Settings

Force HTTPS:

If this option is enabled, access to the web front-end is only possible using a HTTPS connection. The B050-000 will not listen on the HTTP port for incoming connections. In case you want to create your own SSL certificate that is used to identify the B050-000 refer to the Section called Certificate.

KVM encryption:

This option controls the encryption of the RFB protocol. RFB is used by the Remote Console to transmit both the screen data to the administrator machine and keyboard and mouse data back to the host. If set to "Off", no encryption will be used. If set to "Try" the applet tries to make an encrypted connection. In case that the connection cannot be established, an unencrypted connection will be used instead. If set to "Force" the applet tries to make an encrypted connection. An error will be reported in case the connection establishment fails.

Certificate

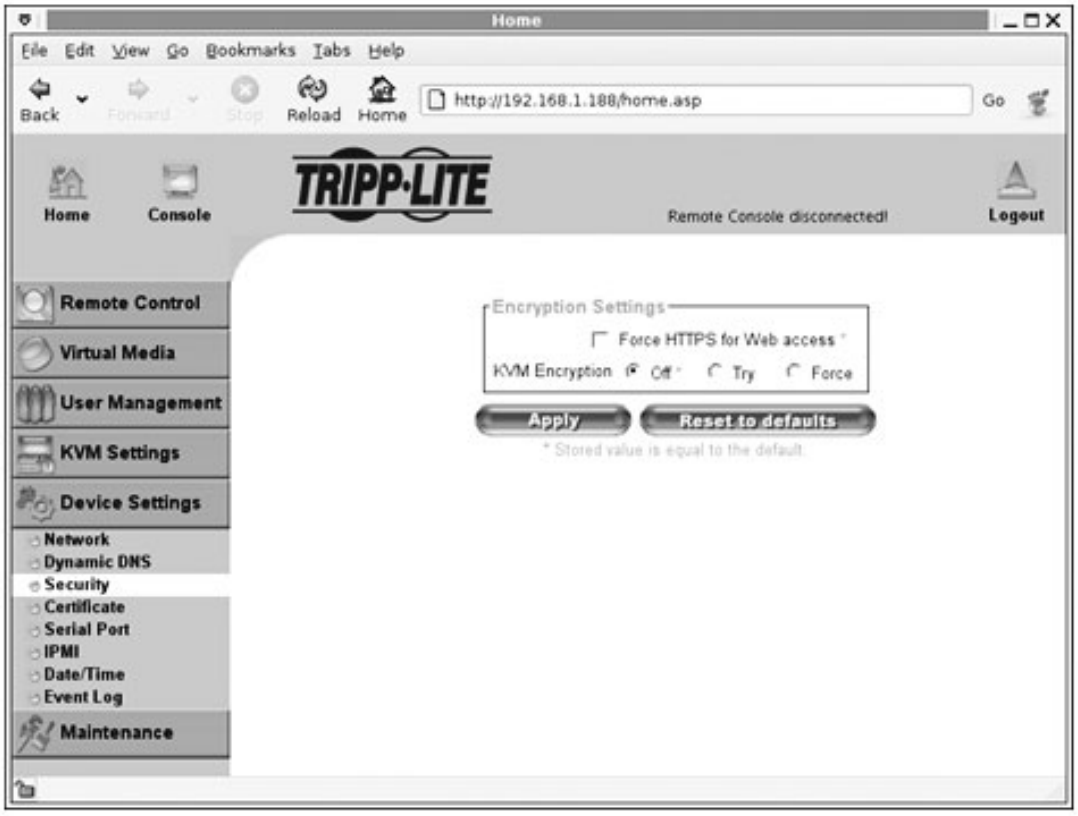


Figure 6-30. Certificate Settings

The B050-000 uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the B050-000 has to expose its identity to a client using a cryptographic certificate. Upon delivery this certificate and the underlying secret key is the same for all B050-000 ever produced and certainly will not match the network configuration that will be applied to the B050-000 by its user. The certificate's underlying secret key is also used for securing the SSL handshake. Hence, this is a security risk (but far better than no encryption at all). However, it is possible to generate and install a new base64 x.509 certificate that is unique for a particular B050-000. In order to do that, the B050-000 is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA). A certification authority verifies that you are the person who you claim you are and signs and issues a SSL certificate to you.
To create and install a SSL certificate for the B050-000 the following steps are necessary:

- Create a SSL Certificate Signing Request using the panel shown in Figure 6-30. You need to fill out a number of fields that are explained below. Once this is done, click on the button “Create” which will initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the”Download CSR” button (see Figure 6-31).

- Send the saved CSR to a CA for certification. You will get the new certificate from the CA after a traditional authentication process (depending on the CA).

• Upload the certificate to the B050-000 using the “Upload” button as shown in Figure 6-31.

Figure 6-31. SSL Certificate Upload

After completing these three steps the B050-000 has its own certificate that is used for identifying the card to its clients.

Warning: If you destroy the CSR on the B050-000, there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described above.

Common name:

This is the network name of the B050-000 once it is installed in the user 's network (usually the fully qualified domain name). It is identical to the name that is used to access the B050-000 with a web browser but without the prefix “http://”. In case the name given here and the actual network name differ, the browser will pop up a security warning when the B050-000 is accessed using HTTPS.

Organizational unit:

This field is used to specifying which department within an organization the B050-000 belongs.

Organization:

The name of the organization to which the B050-000 belongs.

Locality/City:

The city where the organization is located.

State/Province:

The state or province where the organization is located.

Country (ISO code):

The country where the organization is located. This is the two-letter ISO code, e.g. US for the U.S.

Challenge Password:

Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimal length of this password is four characters.

Confirm Challenge Password:

Confirmation of the Challenge Password.

Email:

The email address of a contact person that is responsible for the B050-000 and its security.

Key length:

This is the length of the generated key in bits. 1024 Bits are supposed to be sufficient for most cases. Longer keys may result in slower response time of the B050-000 during connection establishment.

Serial Settings

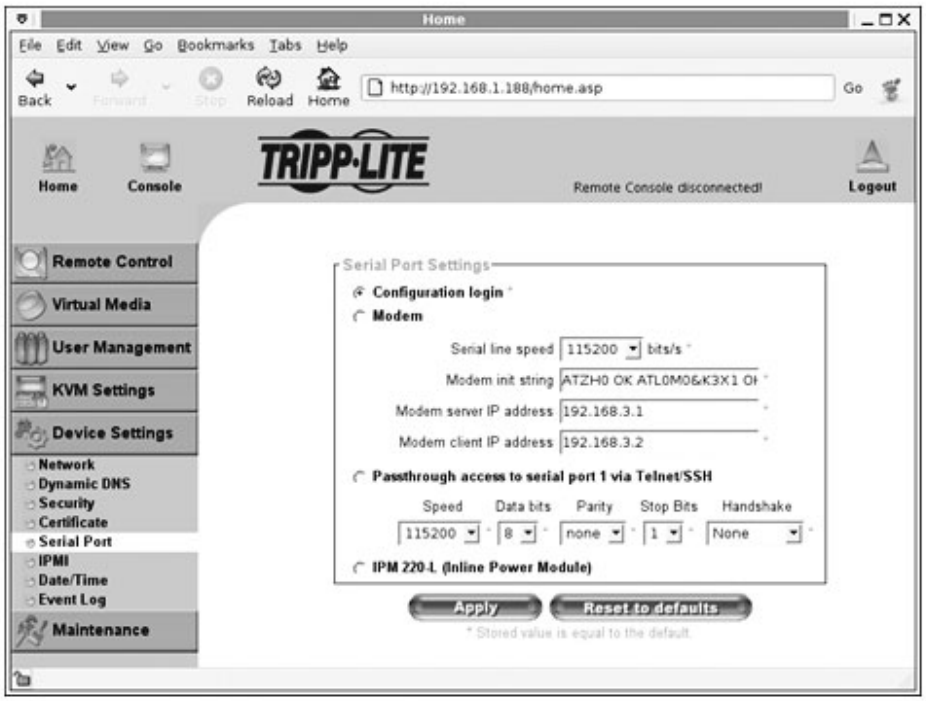


Figure 6-32. Serial Settings

The B050-000 Serial Settings (Figure 6-32) allow you to specify what device is connected to the serial port and how to use it. To access the serial interface a port replicator cable is required (see the Section called B050-000 System Components in Chapter 2).

Configuration or console login:

Do not use the serial port for any special function, use it only for the initial configuration (see Table 4-1).

Modem:

The B050-000 offers remote access using a telephone line in addition to the standard access over the built-in Ethernet adapter. The modem needs to be connected to the serial interface of the B050-000.
Logically, connecting to the B050-000 using a telephone line means nothing else than building up a dedicated point-to-point connection from your console computer to the B050-000. In other words, the B050-000 acts as an Internet Service Provider (ISP) to which you can dial in. The connection is established using the Point-to-Point Protocol (PPP). Before you connect to the B050-000 make sure to configure your console computer accordingly. For instance, on Windows based operating systems you can configure a dial-up network connection which defaults to the right settings like PPP. The Modem Settings panel allows you to configure the remote access to the B050-000 using a modem. The meaning of each parameter will be described below. The modem settings are part of the serial settings panel.

Serial line speed:

The speed with which the B050-000 is communicating with the modem. Most modems available today will support the default value of 115,200 bps. If you are using an old modem and discovering problems try to lower this speed.

Modem Init String:

The initialization string used by the B050-000 to initialize the modem. The default value will work with all modern standard modems directly connected to a telephone line. If you have a special modem or the modem is connected to a local telephone switch that requires a special dial sequence in order to establish a connection to the public telephone network, you can change this setting by giving a new string. Refer to the modem's manual about the AT command syntax.

Modem server IP address:

This IP address will be assigned to the B050-000 itself during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure that it is not interfering with the IP settings of the B050-000 and your console computer. The default value will work in most cases.

Modem client IP address:

This IP address will be assigned to your console computer during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure that it is not interfering with the IP settings of the B050-000 and your console computer. The default value will work in most cases.

Passthrough access to serial port via Telnet/SSH:

Using this option it is possible to connect an arbitrary device to the serial port and access it (assuming it provides terminal support) via Telnet or SSH. Select the appropriate options for the serial port and use the Telnet Console or a standard Telnet/SSH client to connect to the B050-000. For more information about the Telnet interface you may have a look at the Section called Telnet Console.

Intelligent Platform Management Interface (IPMI)

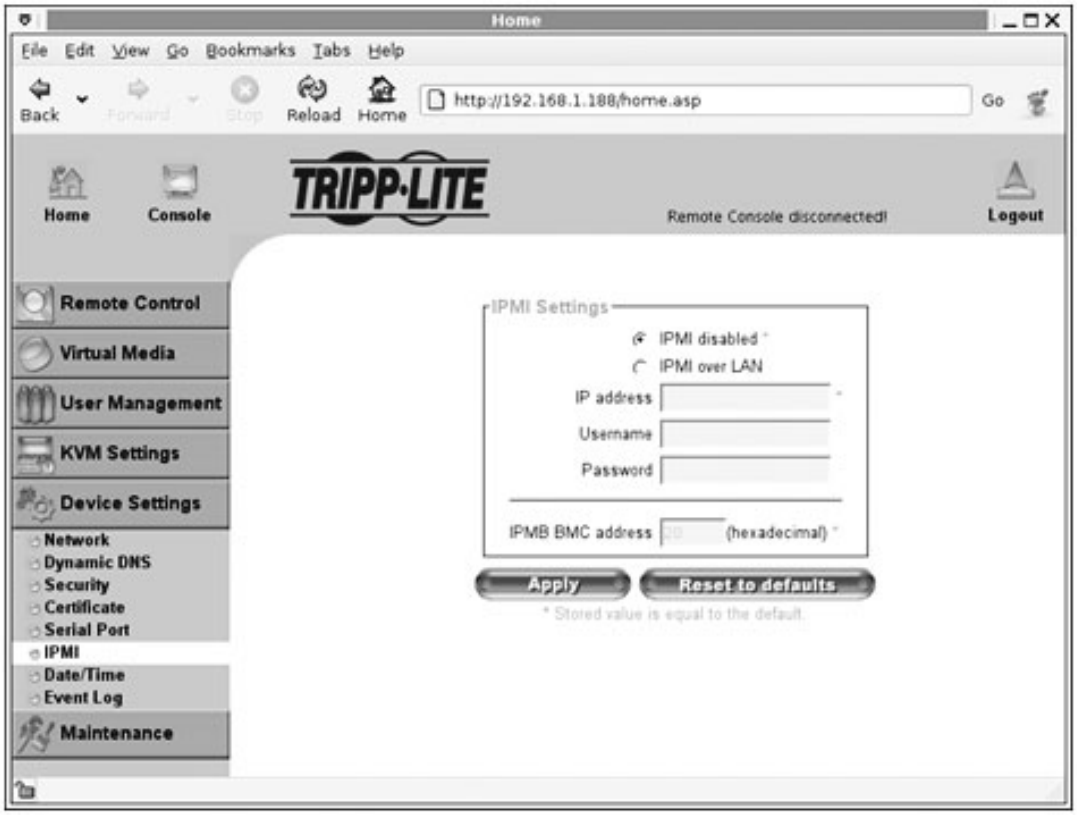


Figure 6-33. IPMI

Generals

You have an additional way to power on or off the system or to perform a hard reset by using the B050-000 IPMI capabilities. It also provides the ability to show an event log of the host system and the status of some system sensors (i.e. temperature). If your host system supports IPMI, you can access it by one of the following ways:

- IPMI over LAN (IPMI V1.5 is required)

6. Menu Options

IPMI Settings

Figure 6-33 shows the B050-000 IPMI settings panel. Its options will be explained below.

IPMI disabled:

Disables IPMI on the B050-000. This means that Status via IPMI and Event Log via IPMI are not available and the power on/off and reset functions do not use IPMI rather than the ATX and the reset cable connected from the B050-000 to the motherboard.

IPMI over LAN:

You can connect the IPMI over a LAN connection, too. The prerequisite for this access type is a host system with IPMI V1.5 and a network adapter with a sideband connection to the BMC (mostly on board). In the IPMI Settings you have to enter the IP address of this host system, the user name of a valid IPMI account and password for this account. You can also access other IPMI systems if you enter their IP address.

Date And Time

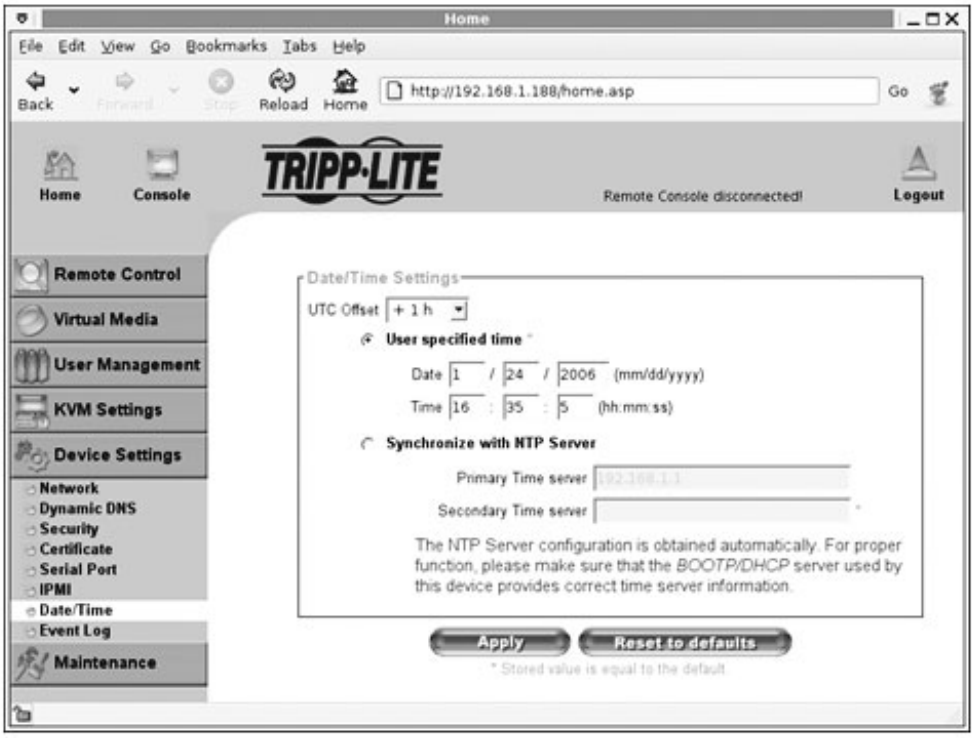


Figure 6-34. Date and Time

This link refers to a page where the internal real time clock of the B050-000 can be set up (see Figure 6-34). You can adjust the clock manually or to use a NTP time server. Without a time server your time setting will not be persistent, so you have to adjust it again after the B050-000 loses power for more than a few minutes. To avoid this you can use a NTP time server which sets up the internal clock automatically to the current UTC time. Because NTP server time is always UTC, there is a setting that allows you to set up a static offset to get your local time.

6. Menu Options

Warning: There is currently no way to adjust the daylight saving time automatically. So you have to set up the UTC offset twice a year properly to the local rules of your country.

Event Log

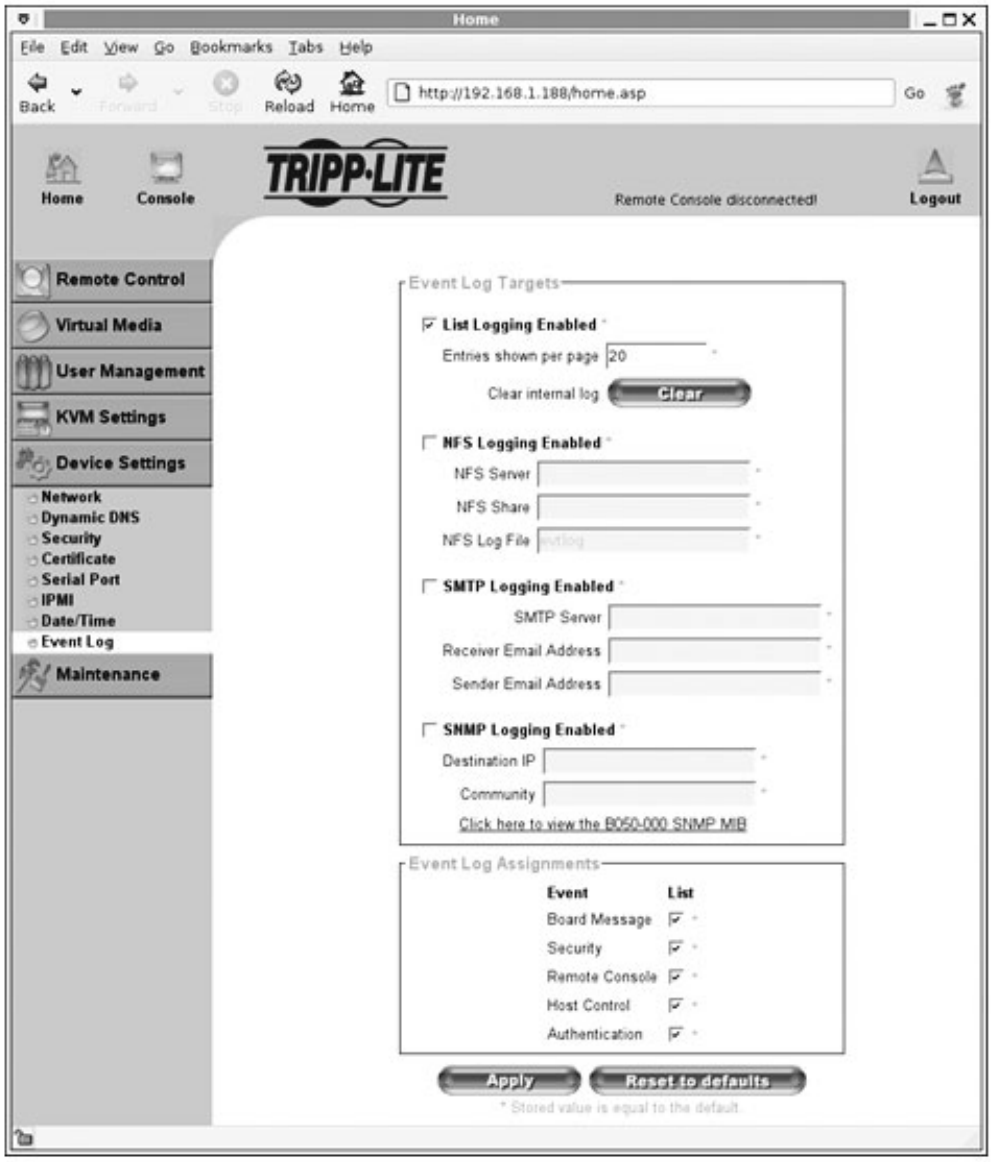


Figure 6-35. Event Log

Important events like a login failure or a firmware update are logged to a selection of logging destinations (see Figure 6-35). Each of those events belong to an event group which can be activated separately.

6. Menu Options

The common way to log events is to use the internal log list of the B050-000. To show the log list click on the item “Event Log” from the section “Maintenance”. In the Event Log Settings you can choose how many log entries are shown on each page. You can also clear the log file here.

Since the B050-000's system memory is used to save all the information, the maximum number of possible log list entries is restricted to 1,000 events. Every entry that exceeds this limit overrides the oldest one automatically.

Warning: If the reset button on the HTML front-end is used to restart the B050-000, all logging information is saved permanently and is available after the B050-000 has been started. If the B050-000 loses power or a hard reset is performed, all logging data will be lost. To avoid this use one of the log methods described below.

NFS Logging enabled:

Define a NFS server where a directory or a static link has to be exported in order to write all logging data to a file that is located there. To write logging data from more than one B050-000 device to only one NFS share, you have to define a file name that is unique for each device. When you change the NFS settings and press the button “Apply”, the NFS share will be mounted immediately. That means the NFS share and the NFS server must be filled with valid sources or you will get an error message.

Warning: In contrast to the internal log file on the B050-000, the size of the NFS log file is not limited. Every log event will be appended to the end of the file so it grows continuously and you may have to delete it or move it away from time to time.

SMTP Logging enabled:

With this option the B050-000 is able to send Emails to an address given by the Email address text field in the Event Log Settings. These mails contain the same description strings as the internal log file and the mail subject is filled with the event group of the occurred log event. In order to use this log destination you have to specify a SMTP server that has to be reachable from the B050-000 device and that needs no authentication at all (<serverip>:<port>).

SNMP Logging enabled:

If this is activated, the B050-000 sends a SNMP trap to a specified destination IP address, every time a log event occurs. If the receiver requires a community string, you can set it in the appropriate text field. Most of the event traps only contain one descriptive string with all information about the log event. Only authentication and host power events have their own trap class that consists of several fields with detailed information about the occurred event. To receive this SNMP traps any SNMP trap listener may be used.

Event Log Assignments

You may choose which actions of the B050-000 will be saved in the log file. Tick the desired box(es) and click “Apply” to confirm your selection.

Maintenance

Device Information

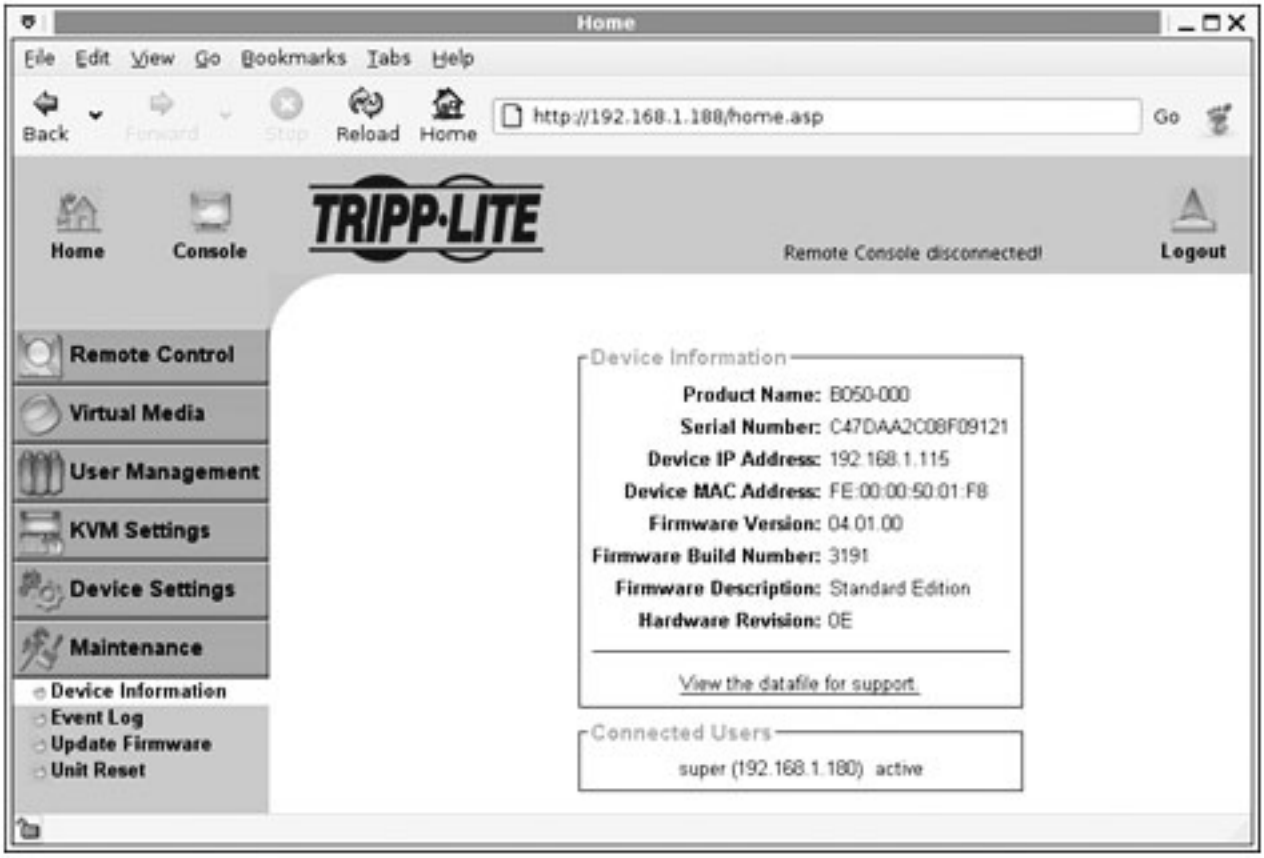


Figure 6-36. Device Information

This section contains a summary with various information about this B050-000 and its current firmware and allows you to reset the device. You may have a look at Figure 6-36 for an example.

The Data file for support allows you to download the B050-000 data file with specific support information. This is an XML file with certain customized support information like the serial number etc. You may send us this information together with a support request. It will help us to locate and solve your reported problem.

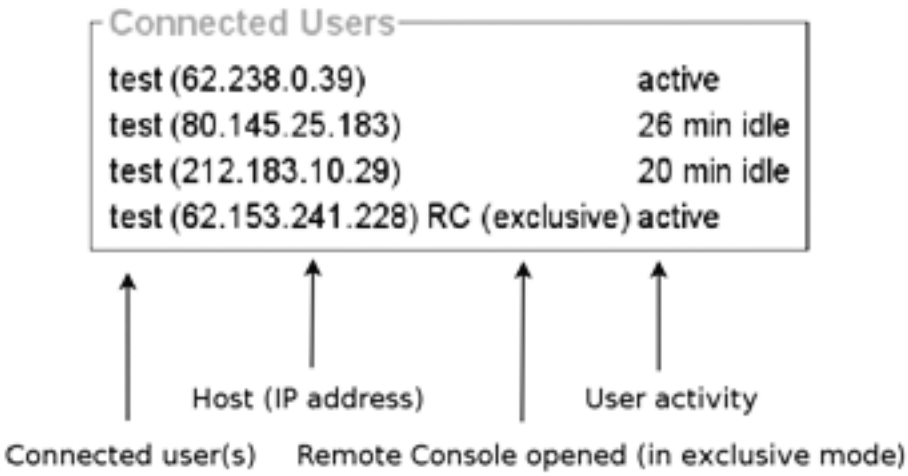


Figure 6-37. Connected Users

Figure 6-37 displays the B050-000 activity. From left to right: the connected user(s), IP address (from which host the user comes from) and activity status are displayed. “RC” indicates that the Remote Console is open. If the Remote Console is opened in “exclusive mode” the term “(exclusive)” is added. For more information about this option see the Section called Remote Console Control Bar in Chapter 5. To display the user activity the last column is used. It contains either the term “active” for an active user or the according idle time for an inactive user.

Event Log

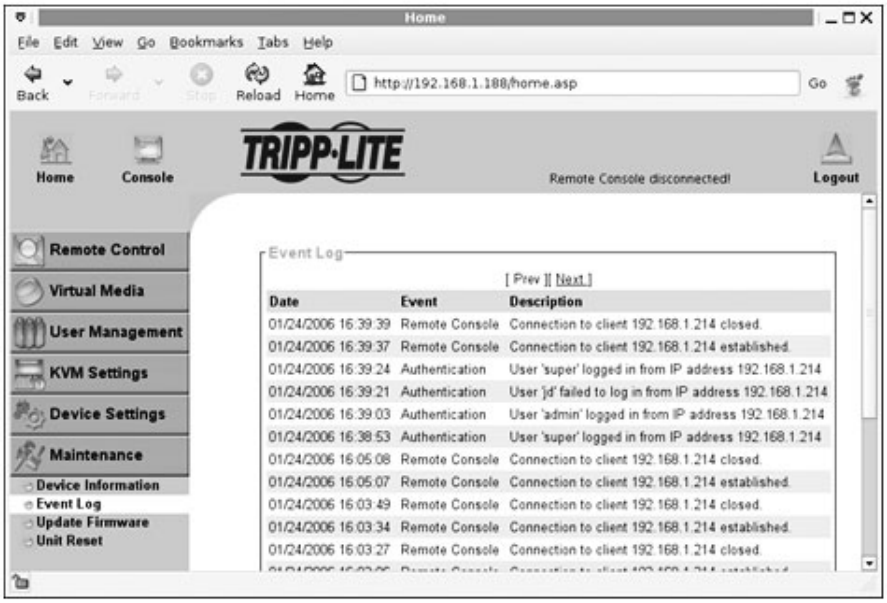

Home
File Edit View Go Bookmarks Tabs Help
Back Forward Stop Reload Home
http://192.168.1.188/home.asp
Go
Home
Console
TRIPP·LITE
Remote Console disconnected!
Logout
Remote Control
Virtual Media
User Management
KVM Settings
Device Settings
Maintenance
Device Information
Event Log
Update Firmware
Unit Reset
Event Log
[Prev][Next]
Date Event Description
01/24/2006 16:39:39 Remote Console Connection to client 192.168.1.214 closed.
01/24/2006 16:39:37 Remote Console Connection to client 192.168.1.214 established.
01/24/2006 16:39:24 Authentication User 'super' logged in from IP address 192.168.1.214
01/24/2006 16:39:21 Authentication User 'jd' failed to log in from IP address 192.168.1.214
01/24/2006 16:39:03 Authentication User 'admin' logged in from IP address 192.168.1.214
01/24/2006 16:38:53 Authentication User 'super' logged in from IP address 192.168.1.214
01/24/2006 16:05:08 Remote Console Connection to client 192.168.1.214 closed.
01/24/2006 16:05:07 Remote Console Connection to client 192.168.1.214 established.
01/24/2006 16:03:49 Remote Console Connection to client 192.168.1.214 closed.
01/24/2006 16:03:34 Remote Console Connection to client 192.168.1.214 established.
01/24/2006 16:03:27 Remote Console Connection to client 192.168.1.214 closed.

Figure 6-38. Event Log List

Figure 6-38 displays the Event Log list. It includes the events that are kept by the B050-000 extended by the event date, a short event description and an IP address from which the request was sent.

You may use the text buttons “Prev” and “Next” to browse within the data. The button “Prev” displays the previous page with newer log information whereas the button “Next” switches to the following page with older log information.

Update Firmware

Figure 6-39. Update Firmware

The B050-000 is a complete standalone computer. The software it runs is called the firmware. The firmware of the B050-000 can be updated remotely in order to install new functionality or special features.
A new firmware update is a binary file, which will be available on www.tripplite.com web site. If the firmware file is a compressed file with suffix .zip you have to unzip it before you can proceed. In order to extract the archive you may use WinZip from http://www.winzip.com/ (for Windows OS) or a tool named unzip that might be already provided in your OS (UNIX, Linux, OS X).
Before you can start updating the firmware of your B050-000, the new and uncompressed firmware file has to be accessible on the system that you use for connecting to the B050-000.

Updating the firmware is a three-stage process:

- Firstly, the new firmware file is uploaded onto the B050-000. In order to do that you need to select the file on your local system using the button “Browse” of the Up- load Firmware panel (see Figure 6-39). Then, click “Upload” to transfer the previously selected file from your local file system onto the B050-000. Once the firmware file has been uploaded, it is checked whether it is a valid firmware file and whether there were any transmission errors. In case of any error the Upload Firmware function will be aborted and the current firmware is kept as is.

- Secondly, if everything went well, you see the Update Firmware panel. The panel shows you the version number of the currently running firmware and the version number of the uploaded firmware. Pressing the button “Update” will store the new version and substitute the old one completely.

Warning: This process is not reversible and might take some minutes. Make sure the B050-000's power supply will not be interrupted during the update process, because this may cause an unusable device.

- Thirdly, after the firmware has been stored, the B050-000 will reset automatically. After about one minute you will be redirected to the Login page and requested to login once again.

Warning: The three-stage firmware update process and complete consistency check make a mistake in updating the firmware almost impossible. However, only experienced staff members or administrators should perform a firmware update. Make sure the B050-000's power supply will not be interrupted!

Unit Reset

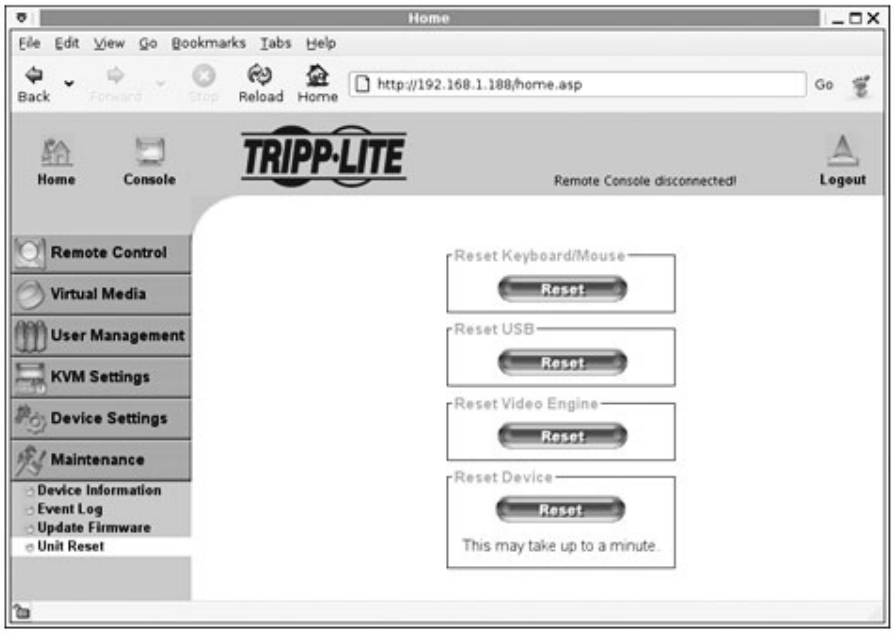


Figure 6-40. Unit Reset

This section allows you to reset specific parts of the device. This involves the both keyboard and mouse, the video engine and the B050-000 itself. Resetting the card itself is mainly needed to activate a newly updated firmware. It will close all current connections to the administration console and to the Remote Console. The whole process will take about half a minute. Resetting subdevices (e.g. video engine) will take a few seconds only and does not result in closing connections. To reset a certain B050-000 functionality click on the button “Reset” as displayed in Figure 6-40.

Note: Only the user “super” is allowed to reset the B050-000.

Appendix A. Frequently Asked Questions

1. The remote mouse does not work or is not synchronous.

First, check the VGA connection. Both the B050-000 and the local monitor have to support the same video resolution. Make sure that your mouse settings match your mouse model, i.e. PS/2 or wheel mouse. The mouse model has to be set similarly on both the B050-000 and the Operating System you use on your host. In some circumstances the mouse synchronization process could behave incorrectly, refer to the Section called Mouse, Keyboard and Video configuration in Chapter 4 for further explanation.

2. The video quality is bad or the picture is grainy.

Enter the Remote Console and press the Auto Adjust button (see the Section called Remote Console Control Bar in Chapter 5) to adjust the B050-000's video input parameters to the correct values.

3. Login on the B050-000 fails.

Verify both your user login and your password. By default, the user “super” has the password “pass”. Moreover, your web browser has to be configured to accept cookies.

4. The Remote Console window of the B050-000 does not open.

A firewall may prevent the access to the Remote Console. The TCP ports #80 (for HTTP) and #443 (for both HTTPS and RFB) have to be open (the server providing the firewall has to accept incoming TCP connections on these ports).

5. Remote console is unable to connect and displays a timeout error.

Have a look on your hardware. If there is a proxy server between the B050-000 and your host, then you may not be able to transfer the video data using RFB. Establish a direct connection between the B050-000 and the client. Furthermore, check the settings of the B050-000 and choose a different server port used for RFB transfer. If you use a firewall then check the according port for accepting connections. You may restrict these connections for the IP addresses used by the B050-000 and your client.

6. No connection can be established to the B050-000.

Have a look on your hardware. Is the B050-000 attached to a power supply? Verify your network configuration (IP address, router). You may send a “ping” request to the B050-000 to find out whether the B050-000 is reachable via network.

7. Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.

You have to define a so-called “Button Key”. This can be done in the Remote Console settings (see the Section called Remote Console Control Bar in Chapter 5). Alternatively you can use the soft keyboard feature (see the Section called Soft Keyboard in Chapter 5).

Appendix A. Frequently Asked Questions

8. The B050-000 web pages are not displayed correctly.

Check your browser 's cache settings. Make sure the cache settings are not set to something like “never check for newer pages”. Otherwise the B050-000 pages may be loaded from your browser cache and not from the card.

9. Windows XP does not awake from standby mode.

This is possibly a Windows XP problem. Try not to move the mouse pointer while XP switches into standby mode.

10. For SUN computers a USB keyboard does not work.

The B050-000 emulates a USB keyboard. If you attach a USB keyboard to your host two keyboards are detected. It cannot be predicted which one of these comes first and you will be able to work with. SUN supports only one USB keyboard.

11. Cannot upload the signed certificate in MacOS X.

If an “internal error” occurs while uploading the signed certificate, either change the extension of the file to .txt or add a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is set to “plain text” and the checkbox “use for outgoing” is set. As an alternative, you may also use a Mozilla based browser (Mozilla, FireFox).

12. Every time I open a dialog box with some buttons the mouse pointers are not synchronous anymore.

Disable the setting “Automatically move mouse pointer to the default button of dialog boxes” in the mouse settings of your operating system.

13. The Remote Console does not open with Opera in Linux.

Some versions of Opera do not grant enough permissions if the signature of the applet cannot be verified. To solve the problem, add the lines grant codeBase “nn.pp.rc.RemoteConsoleApplet” {permission java.lang.RuntimePermission “accessClassInPackage.sun.*”; to the java policy file of opera (e.g. /usr/share/opera/java/opera.policy).

14. The Remote Console remains black.

Check if the B050-000 is being USB powered only. If there is not enough power via USB, the remote Console opens but remain black. Attach the external power supply to the B050-000. Verify the B050-000 settings using the according section in the front end.

15. I forgot my password. How can I reset the B050-000 to factory defaults?

You may use the serial interface. For a detailed description see the Section called “Resetting the B050-000 to its Factory Settings” in Chapter 4.

Appendix B. Glossary

ACPI—Advanced Configuration and Power Interface

A specification that enables the operating system to implement power management and system configuration.

ATX—Advanced Technology Extended

A particular specification that covers the style of motherboards and enclosure introduced by Intel in 1995.

DHCP—Dynamic Host Configuration Protocol

A protocol for dynamically assigning IP configurations to host names, especially used in a local network.

DNS—Domain Name System

A protocol used to locate computers on the Internet by their name.

FAQ—Frequently Asked Questions

HTTP—Hypertext Transfer Protocol

One of the protocols used for communication between single computers, especially between web browsers and web servers.

HTTPS—Hypertext Transfer Protocol Secure

The secure version of HTTP.

IPMI—Intelligent Platform Management Interface

A specification defining a set of common interfaces for operating system independent platform management and health monitoring.

LED—Light Emitting Diode

A semiconductor device that emits incoherent monochromatic light when electrically biased in the forward direction.

PS/2—Personal System/2

IBM's second generation of personal computers, which was released to the public in 1987. Today, PS/2 is known as a device interface for mouse and keyboard.

Appendix B. Glossary

SNMP—Simple Network Management Protocol

A widely used network monitoring and control protocol.

SSH—Secure Shell

An encrypted network protocol providing a secure replacement for Telnet.

SSL—Secure Socket Layer

An encryption technology for the Internet used to provide secured data transmissions.

SVGA—Super Video Graphics Array

A refinement of the Video Graphics Array (VGA) that provides increased pitch and resolution performance.

UTP—Unshielded Twisted Pair

A cable with two conductors twisted as a pair and bundled within the same outer PVC covering.

Appendix C. B050-000 Video Modes

Table C-1 lists the video modes the B050-000 supports. Please do not use any other custom video settings besides of these. If done so, the B050-000 may not be able to detect them.

Resolution (x,y)	Refresh Rates (Hz)
640x340	70, 85
640x400	56, 85
640x480	60, 67, 72, 75, 85, 90, 100, 120
720x400	70, 85
800x600	56, 60, 70, 72, 75, 85, 90, 100
832x624	75
1024x768	60, 70, 72, 75, 85, 90, 100
1152x864	75
1152x870	75
1152x900	66, 76
1280x960	60, 85
1280x1024	60, 75, 85
1600x1200	60, 65, 70, 75
2048x1536	85 (local port only)

Table C-1. B050-000 Video Modes

Appendix D. Users and Roles

Table D-1. Roles

Frontend Section	Regular User	Administrator	Superuser
Remote Control: KVM	x	x	x
Remote Control: Remote Power	x	x	x
Remote Control: Telnet Console	x	x	x
Virtual Media	x	x	x
User Management: Change Password	x	x	x
User Management: Users	—	—	x
KVM Settings: User Console	x (w/o Misc. Settings)	x	x
KVM Settings: Keyboard/Mouse	—	x	x
KVM Settings: Video	—	x	x
Device Settings	—	—	x
Maintenance: Device Information	x	x	x
Maintenance: Event Log	—	—	x
Maintenance: Update Firmware	—	—	x
Maintenance: Unit Reset	Keyboard/ Mouse, Video	Keyboard/ Mouse, Video	Keyboard/ Mouse, Video, Device

Appendix E. Key Codes

Table E-1 shows the key codes used to define the key strokes or hotkeys for several functions. Please note that these key codes do not necessarily represent the key characters that are used on international keyboards. A key on a standard 104 key PC keyboard with a US English language mapping is named. The layout for this keyboard is shown in Figure E-1. However, most modifier keys and other alphanumeric keys used for hotkey purposes in application programs are on a similar position, no matter what language mapping you are using. Some of the keys also have aliases. This means that a key can be named by two different key codes.

Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Prnt Scrl Brk
~ 1 2 3 4 5 6 7 8 9 0 - = Bsp Ins Pos1 Pgup Num / * -
tab q w e r t y u i o p [ ] CR Del End Pgdn 7 8 9 +
Caps a s d f g h j k l ; ' \ 4 5 6
LShift z x c v b n m , . ? Rshift Up 1 2 3 CR
Lctrl Win Alt Space AltGR Menu RCtrl Left Down Right 0 ,

Figure E-1. English (US) keyboard Layout, used for the key codes

Table E-1. Key Names

Key	Alias Key(s)
0 - 9	
A - Z	
~	TILDE
_	MINUS
=	EQUALS
;	
'	
<	LESS
,	
.	
/	SLASH BACKSPACE
TAB	
[	
]	
ENTER	
CAPS LOCK	
\	BACK SLASH
LSHIFT	SHIFT
RCTRL	CTRL, STRG
RSHIFT	SHIFT
LCTRL	CTRL, STRG

Appendix E. Key Codes

Key	Alias Key(s)
LALT	ALT
SPACE ALT GR	
ESCAPE	ESC
F1	
F2	
F3	
F4	
F5	
F6	
F7	
F8	
F9	
F10	
F11	
F12	
PRINTSCREEN	
SCROLL LOCK	
BREAK	
INSERT HOME	POS 1
PAGE_UP	
PAGE_DOWN	
DELETE	DEL
END	
UP	
LEFT	
DOWN	
RIGHT	

Key	Alias Key(s)
NUM_LOCK	
NUMPAD0	
NUMPAD1	
NUMPAD2	
NUMPAD3	
NUMPAD4	
NUMPAD5	
NUMPAD6	
NUMPAD7	
NUMPAD8	
NUMPAD9	
NUMPADPLUS	NUMPAD_PLUS, +
NUMPAD /	/
NUMPADMUL	NUMPAD_MUL,
NUMPADMINUS	NUMPAD_MINUS,
NUMPADENTER	
WINDOWS MENU	

Appendix F. Pin Assignment

VGA HD-15

Figure F-1. VGA HD-15

Table F-1. VGA HD-15

Pin	Assignment	Pin	Assignment
1	Red	9	USB+5V
2	Green	10	GND sync
3	Blue	11	USB_D+
4	USB_D -	12	SDA, DDC...
5	GND	13	HSYNC
6	GND red	14	VSYNC
7	GND green	15	SCL, DDC
8	GND blue		

RJ45 Connector Ethernet

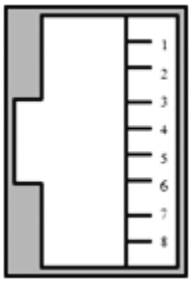


Figure F-2. RJ45

Table F-2. RJ45

Pin	Assignment	Pin	Assignment
1	TX +	5	Not connected
2	TX -	6	RX-
3	RX +	7	Not connected
4	Not connected	8	Not connected

Appendix G. Specifications

Sizes and Weight

Table G-1. B050-000 Specification

Attribute	Value
Height	95mm
Width	25mm
Length	72mm
Weight	160g (w/o replicator cable)
	290g (with attached replicator cable)
Housing	Aluminium silver anodized
Power Consumption	up to 700mA

Environment

Temperature

Table G-2. Temperature

Attribute	Value
Operating	0? C to 55? C (32? F to 131? F)
Storage	-18? C to 70? C (-0.4? F to 158? F)

Humidity

Table G-3. Humidity

Attribute	Value
Operating	10% to 90% (non-condensing)
Storage	5% to 95% (non-condensing)

Appendix H. B050-000 Operation Advice

This device has to be operated with the provided power supply only. The use of other power supplies voids the product liability of the manufacturer. If the power supply shows a malfunction, it must not be opened.

The power cord of the power supply is the point of junction to the supply network AC 230 V. Therefore both the power supply and the socket have to be easily accessible to disconnect them quickly if it is necessary.

Appendix I. FCC Statement

FCC Radio/TV Interference Notice

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. The user must use shielded cables and connectors with this product. Any changes or modifications to this product not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Appendix J: Tripp Lite Warranty Information

1-Year Limited Warranty

TRIPP LITE warrants its products to be free from defects in materials and workmanship for a period of one (1) year from the date of initial purchase. TRIPP LITE's obligation under this warranty is limited to repairing or replacing (at its sole option) any such defective products. To obtain service under this warranty, you must obtain a Returned Material Authorization (RMA) number from TRIPP LITE or an authorized TRIPP LITE service center. Products must be returned to TRIPP LITE or an authorized TRIPP LITE service center with transportation charges prepaid and must be accompanied by a brief description of the problem encountered and proof of date and place of purchase. This warranty does not apply to equipment, which has been damaged by accident, negligence or misapplication or has been altered or modified in any way.

EXCEPT AS PROVIDED HEREIN, TRIPP LITE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Some states do not permit limitation or exclusion of implied warranties; therefore, the aforesaid limitation(s) or exclusion(s) may not apply to the purchaser.

EXCEPT AS PROVIDED ABOVE, IN NO EVENT WILL TRIPP LITE BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS PRODUCT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Specifically, TRIPP LITE is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, costs of substitutes, claims by third parties, or otherwise.

Warranty Registration

Visit www.tripplite.com/warranty today to register the warranty for your new Tripp Lite product. You'll be automatically entered into a drawing for a chance to win a FREE Tripp Lite product!*

* No purchase necessary. Void where prohibited. Some restrictions apply. See website for details.

The policy of TRIPP LITE is one of continuous improvement. Specifications are subject to change without notice.

Tripp Lite World Headquarters
1111 W. 35th Street, Chicago, IL 60609 USA
(773) 869-1234 • www.tripplite.com

200605171 93-2563